UNITED STATES ARMY WAR COLLEGE PRESS
Carlisle Barracks, PA
STRENGTH and WISDOM

MAINTAINING INFORMATION DOMINANCE IN COMPLEX ENVIRONMENTS

John A. S. Ardis
Shima D. Keene

U.S. ARMY WAR COLLEGE
SSI
STRATEGIC STUDIES INSTITUTE

The United States Army War College

The United States Army War College educates and develops leaders for service at the strategic level while advancing knowledge in the global application of Landpower.

The purpose of the United States Army War College is to produce graduates who are skilled critical thinkers and complex problem solvers. Concurrently, it is our duty to the U.S. Army to also act as a "think factory" for commanders and civilian leaders at the strategic level worldwide and routinely engage in discourse and debate concerning the role of ground forces in achieving national security objectives.

The Strategic Studies Institute publishes national security and strategic research and analysis to influence policy debate and bridge the gap between military and academia.

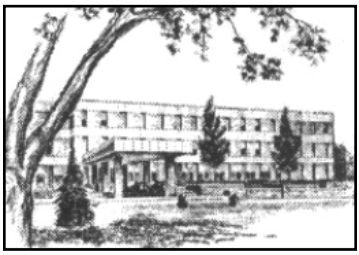
The Center for Strategic Leadership contributes to the education of world class senior leaders, develops expert knowledge, and provides solutions to strategic Army issues affecting the national security community.

The Peacekeeping and Stability Operations Institute provides subject matter expertise, technical review, and writing expertise to agencies that develop stability operations concepts and doctrines.

The School of Strategic Landpower develops strategic leaders by providing a strong foundation of wisdom grounded in mastery of the profession of arms, and by serving as a crucible for educating future leaders in the analysis, evaluation, and refinement of professional expertise in war, strategy, operations, national security, resource management, and responsible command.

The U.S. Army Heritage and Education Center acquires, conserves, and exhibits historical materials for use to support the U.S. Army, educate an international audience, and honor Soldiers—past and present.

STRATEGIC STUDIES INSTITUTE



The Strategic Studies Institute (SSI) is part of the U.S. Army War College and is the strategic-level study agent for issues related to national security and military strategy with emphasis on geostrategic analysis.

The mission of SSI is to use independent analysis to conduct strategic studies that develop policy recommendations on:

- Strategy, planning, and policy for joint and combined employment of military forces;
- Regional strategic appraisals;
- The nature of land warfare;
- Matters affecting the Army's future;
- The concepts, philosophy, and theory of strategy; and,
- Other issues of importance to the leadership of the Army.

Studies produced by civilian and military analysts concern topics having strategic implications for the Army, the Department of Defense, and the larger national security community.

In addition to its studies, SSI publishes special reports on topics of special or immediate interest. These include edited proceedings of conferences and topically oriented roundtables, expanded trip reports, and quick-reaction responses to senior Army leaders.

The Institute provides a valuable analytical capability within the Army to address strategic and other issues in support of Army participation in national security policy formulation.

Strategic Studies Institute
and
U.S. Army War College Press

MAINTAINING INFORMATION DOMINANCE IN COMPLEX ENVIRONMENTS

John A. S. Ardis
Shima D. Keene

October 2018

The views expressed in this report are those of the authors and do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, or the U.S. Government. Authors of Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press publications enjoy full academic freedom, provided they do not disclose classified information, jeopardize operations security, or misrepresent official U.S. policy. Such academic freedom empowers them to offer new and sometimes controversial perspectives in the interest of furthering debate on key issues. This report is cleared for public release; distribution is unlimited.

*****

This publication is subject to Title 17, United States Code, Sections 101 and 105. It is in the public domain and may not be copyrighted.

*****

Comments pertaining to this report are invited and should be forwarded to: Director, Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, 47 Ashburn Drive, Carlisle, PA 17013-5238.

*****

This manuscript was funded by the U.S. Army War College External Research Associates Program. Information on this program is available on our website, *http://ssi.armywarcollege.edu/*, at the Opportunities tab.

*****

All Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press publications may be downloaded free of charge from the SSI website. Hard copies of certain reports may also be obtained free of charge while supplies last by placing an order on the SSI website. Check the website for availability. SSI publications may be quoted or reprinted in part or in full with permission and appropriate credit given to the U.S. Army Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, Carlisle, PA. Contact SSI by visiting our website at the following address: *http://ssi.armywarcollege.edu/*.

*****

The Strategic Studies Institute and U.S. Army War College Press publishes a quarterly email newsletter to update the national security community on the research of our analysts, recent and forthcoming publications, and upcoming conferences sponsored by the Institute. Each newsletter also provides a strategic commentary by one of our research analysts. If you are interested in receiving this newsletter, please subscribe on the SSI website at the following address: *http://ssi.armywarcollege.edu/newsletter/*.

ISBN 1-58487-790-1

FOREWORD

In the information domain, the U.S. Army is an attractive target for adversary commanders and fighters, terrorist groups, and disaffected individuals. There are many risks to Army command and control (C2) operations and to intelligence and information warfare (IW) capabilities. Challenges are likely to include: significant uncertainty; sudden unexpected events; high noise and clutter levels in intelligence pictures; basic and complex deceptions exercised through a variety of channels; the actions of hidden malign actors; and novel forms of attack on U.S. and allied command, control, communications, computers, information/intelligence, surveillance, targeting acquisition, and reconnaissance (C4ISTAR) systems.

Dr. John A. S. Ardis and Dr. Shima D. Keene have between them many years' experience in intelligence, counterintelligence, counterterrorism, and scientific innovation. In this monograph, the authors explore the risks and instabilities that could threaten the U.S. Army's control of the complex informational and physical environments. They argue that the complexities and uncertainties of the environments are legitimate and perennial characteristics of an increasingly connected world. They suggest that the U.S. Army should seek to exploit complexity and uncertainty and not simply try to overcome it using technical intelligence and human sources. To achieve such exploitation will require rich innovation, extensive training, rigorous testing, and expert integration and coordination.

The authors put forward concepts for special information operations (SIO) that are appropriate for the forthcoming challenges. They highlight the value of

developing an advanced counterintelligence capability and introduce the concepts of signature warfare, sublime operations, and other novel techniques.

To achieve and maintain information dominance, the U.S. Army must adapt, learn, and develop. This monograph contributes to that development by identifying risks and proposing mitigations that can provide operational advantage.

DOUGLAS C. LOVELACE, JR.
Director
Strategic Studies Institute and
U.S. Army War College Press

ABOUT THE AUTHORS

JOHN ARDIS is a British scientist with 25 years of experience in defense, security, and intelligence. He is presently a senior analyst within the United Kingdom (UK) Government and the special operations lead for the Over-Watch Maritime Security Group. He has worked in the United States, Europe, Israel, and the Middle East. He was an associate senior research fellow at the UK Defence Academy's Advanced Research and Assessment Group from 2006-2007. He has worked in defense acquisition on a series of major projects for the British Army, the Royal Navy, the Royal Air Force, and British Joint Services. He has also worked on the development of the UK's Strategic Deterrent program. Dr. Ardis helped develop and run exercises on land for dismounted close combat, and at sea in the Pacific and Mediterranean, specializing in anti-submarine warfare, while playing an active role in the UK's Maritime Technical Intelligence Committee.

Dr. Ardis has provided support to operations in Afghanistan, developing a new improvised explosive device detection system (members of the team were all commended by the UK Ministry of Defence [MoD] Chief Scientific Advisor). He helped train the Iraqi National Security Council in the implementation of the Baghdad Security Plan in 2007 with senior UK and U.S. staff. Dr. Ardis has worked at, and delivered classified operational products to the UK's Permanent Joint Headquarters at Northwood, London. He has worked on various projects in the Defence Intelligence Staff headquarters, and devised and delivered the UK's information warfare catalogue to Operation HERRICK (the British military deployment to Afghanistan) at the highest priority instruction of the UK's Chief of Defence Staff.

Dr. Ardis has lectured at the London Stock Exchange, numerous conferences, and at 15 (UK) Psychological Operations Group on complex information operations and advanced counterintelligence. Dr. Ardis has published reports on cyber problem analysis. He holds an honors degree in computational physics and a doctorate in intelligence and deception operations.

SHIMA D. KEENE is a British academic and practitioner specializing in defense and security. She is a director of the Conflict Studies Research Centre, Oxford, and a senior fellow at the Institute for Statecraft, London. Dr. Keene is also a deployable civilian expert for the UK Government's Civilian Stabilisation Group, specializing in intelligence and security sector reform within the security and justice function. She is a former senior research fellow and advisor at the UK Defence Academy's Advanced Research and Assessment Group, and special advisor to the UK MoD, where she had responsibility for assessing and developing recommendations for financial counterinsurgency strategies in Afghanistan. Dr. Keene advises and works closely with a number of UK Government departments and law enforcement agencies to include the MoD, Foreign and Commonwealth Office, Home Office, Department for International Development, and the National Crime Agency, as well as a number of regional law enforcement agencies. Outside the UK, she works with international organizations to include the Organization for Security and Co-operation in Europe, the Council of Europe, and the North Atlantic Treaty Organization (NATO), as well as the U.S. military, government departments, and law enforcement agencies. She has 26 years of practitioner experience obtained through investment banking, defense intelligence and

academia, and is a former British Army Reservist soldier with 7 years of military service, most of which was spent with 4th Battalion, the Parachute Regiment.

Dr. Keene has published numerous internal and external government and corporate reports, as well as award-winning academic journal articles. She is the author of *Threat Finance: Disconnecting the Lifeline of Organized Crime and Terrorism* and a book chapter in the *Research Handbook on International Financial Crime*. She is a visiting lecturer at the BPP Law School, London, UK, and the Centre for Development Studies, Cambridge University, Cambridge, UK. Dr. Keene holds a Ph.D. in international criminal law, an M.Phil. in defence and security studies, and graduated with honors in business studies.

SUMMARY

The U.S. Army is committed to a high state of resilience and readiness. The problem is that for complex environments, the U.S. Army cannot afford simply to be very effective in a known set of circumstances and unprepared for others, and neither can it afford to be no more than moderately capable in the broadest possible range of circumstances. The U.S. Army has to be effective across the board, and that places extraordinary demands on its Soldiers during all phases of preparation for and engagement in conflict.

Dominance in the information space is a critical capability that will enable the U.S. Army to determine if, how, and when it will engage in conflict. For the U.S. Army to achieve and maintain information dominance, it will have to advance its capabilities to the point where it can rapidly and effectively deploy capabilities that outmaneuver advanced, well-resourced, and unconstrained threats under very difficult circumstances. This will require innovation, planning, and resilience, allowing its information capabilities to survive complex, premeditated, and asymmetric attack. In addition to deploying advanced information related capabilities (IRCs), the U.S. Army has to protect its own capabilities (including those of joint forces and allies) while degrading the adversary's capabilities.[1]

This monograph explores some example risks and suggests that, when combating an unconstrained adversary, training and preparing a suite of novel and tested operations is a necessary complement to the U.S. Army's current warfighting capabilities.

The risks to information dominance are varied. Examples include the likelihood that potential adversaries are already committed to aggressive infor-

mation activities ranging from elementary deception operations to the nuanced use of multiple channels to achieve information and physical sabotage. It is also likely that there will be a further proliferation of communications and cyber technologies allowing nations, terrorist groups, and even individuals to corrupt, jam, and spoof U.S. Army communications; interrupt the supply chain; and possibly degrade command and control systems.

The tempo of information warfare may increase to the point where the mean time between significant events is shorter than the time needed to generate rational decisions or resolve ambiguities. This will challenge even the most expert decision-maker. Some nations will field highly protected special capabilities, so the U.S. Army will have to account for advanced information warfare methods and systems in the Joint Plan, even when the adversary's capabilities are unknown. It may also be increasingly challenging for all participants to discriminate between real and decoy physical targets in congested and noisy environments—even with advanced sensors.

In order to achieve and maintain information dominance, the U.S. Army must exploit the complexity and uncertainty of the battlespace and not simply seek to overcome it. As part of this venture, the U.S. Army must be prepared to field robust and potentially complex deceptions in support of its strategic objectives—enough to overmatch the adversary's counter-deception capabilities.

The U.S. Army's prowess in conventional warfighting should be augmented by the exploitation of a variety of advanced special operations in the technological and informational domains, expertly and rapidly integrated, using multiple tested outcome strat-

egies that will survive and succeed under uncertain and very aggressive circumstances. The proficient use of special information operations (SIO) will create cumulative effects, where each operation magnifies the effect of those already undertaken, and prepares the ground for subsequent operations. SIO are particularly useful when the commander wishes to put the adversary on the back foot, and, as such, they are one of the most cost-effective and low-risk means by which the U.S. Army can achieve and maintain information dominance.

The U.S. Army should field a strong tactical and operational level active counterintelligence capability that deliberately targets adversary intelligence functions and undertakes various activities to mislead and degrade them. In particular, we note that the U.S. Army's existing integration staff within the Army Capabilities Integration Center (ARCIC) are pivotal in the process of coordinating the significant conventional warfighting and information capabilities along with additional special capabilities.[2] The integration process exists in the preparatory stages (led by ARCIC), and also during conflict (within the U.S. Army and at the joint level). We present recommendations that will support the U.S. Army's need to seize the initiative and deploy coordinated operations that protect its assets and Soldiers, and manipulate and penetrate the mind of the adversary commander, leaving him confused and ineffective.

ENDNOTES - SUMMARY

1. Headquarters, Department of the Army, *Information Operations*, Field Manual 100-6, Washington, DC: U.S. Government Printing Office, August 1996, pp. 1-9.

2. The Army Capabilities Integration Center's (ARCIC) role is defined in the U.S. Army Training and Doctrine Command (TRADOC), U.S. Department of the Army, *Concept Development, Capabilities Determination, and Capabilities Integration*, TRADOC Pamphlet 71-20, Joint Base Langley-Eustis, VA: U.S. Army Training and Doctrine Command, June 28, 2013, p. 16.

MAINTAINING INFORMATION DOMINANCE IN COMPLEX ENVIRONMENTS

INTRODUCTION

Despite being over 20 years old, the U.S. Army's definition of information dominance from 1996 remains valid. It is defined as:

> the degree of information superiority that allows the possessor to use information systems and capabilities to achieve an operational advantage in a conflict or to control the situation in operations short of war, while denying those capabilities to the adversary.[1]

The U.S. Army is well-positioned to seize the initiative and develop sustainable measures that will support its role as the leading component of a coordinated information operations (IO) force. In order for the U.S. Army to exercise advantage through information dominance, its key underlying concepts, characteristics, risks, and opportunities, need to be fully appreciated and analyzed. A program of innovation and analysis should be implemented in order to equip the future commander with the options to overmatch adversaries in all environments.

This monograph explores some example risks and suggests that, when combating an unconstrained adversary, the preparation of a suite of novel and tested operations will complement the U.S. Army's warfighting capabilities. The environments may be congested and all participants will be subject to significant forms of uncertainty, but the U.S. Army should exploit the complexity and uncertainties by being able to rapidly deploy operations that prevent the adversary from functioning and making rational decisions.

PART 1: EMERGING CHALLENGES

Information dominance has three main applications: command and control (C2), defense intelligence, and information warfare (IW).[2] C2 enables everyone to know where they and their cohorts are in the battlespace, and allows them to execute operations promptly when necessary. Defense intelligence ranges from knowing the enemy's dispositions to knowing the location of enemy assets in real time with sufficient precision for a one-shot kill. IW confounds enemy information systems at various points (sensors, communications, processing, and command), while protecting one's own. The ultimate target of IW is the information dependent process.[3] The U.S. Army needs to deploy information related capabilities (IRCs) in support of its objectives and protect its own capabilities, while degrading the adversary's capabilities.

Technologies and Proliferation

The pace of technological advancements in recent years has resulted in the erosion of military dominance in the information technology domain. Potential and actual adversaries are beginning to develop offensive and defensive IRCs that rival, and in some cases, surpass those of the U.S. Army. As technologies become more available and affordable, adversary tactics could evolve to exploit asymmetric advantages, gaining advantage over conventional modes of operation. Adversaries will employ the full range of emerging technologies in warfare to include cyber and advanced electronic warfare.[4] For example, North Korea's interest in cyberattacks, malware, and espionage is of particular concern to South Korea as well as

the United States. North Korea also reportedly undertakes ambitious hacking to subvert and deny services in other countries.[5] For adversaries, IW can provide a rapid and cost effective advantage because it is generally perceived as an accessible weapon.

Additionally, with the proliferation of communications technologies and the attractiveness of information as a ubiquitous lever or weapon, the information environment and the electromagnetic spectrum have become congested and cluttered. The Defense Advanced Research Projects Agency (DARPA) is seeking proposals to help contain the risks, but on a global scale, a lack of regulation may cause persistent interference.[6] As a result, it has become increasingly difficult to verify the success or failure of information activities. Many groups and individuals clamor to promote their own views and messages to a diverse audience, using Internet connectivity, social media, and encrypted smartphones encouraging an accelerating tempo of exchange and coordination of action. The result is that it has become increasingly difficult to prevent the flow of adversary intelligence and communications. The Islamic State in Iraq and Syria (ISIS), for example, uses off-the-record protocols, meaning that it has end-to-end encryption at low cost, between multiple parties, using mobile phones as platforms. Friendly intelligence agencies can obtain the communications metadata, but the messages themselves may be inaccessible.[7]

New technologies help us understand what communications are being used and can provide valuable access and insight. However, in times of major upheaval, the sheer bulk of encrypted and open communications threatens to overwhelm media and intelligence services. A case is point was the "Arab Spring"

uprising where events moved so quickly in a short period of time that it was not possible to anticipate outcomes with any degree of certainty.[8]

The Complex Environment

> Complexity and rapid change characterize today's strategic environment, driven by globalization, the diffusion of technology, and demographic shifts.[9]

The information environment and the physical environment are both complex, making the task of measuring the effects of IO even harder.[10] This complexity also challenges the U.S. Army's intelligence and counterintelligence processes by providing cover for adversary activities, such as the infiltration of industry and commercial organizations.[11]

Adversaries may exploit multiple lines of communication and develop bespoke intelligence channels that are hard to intercept. At the same time, socio-technical events in the areas of interest may provide erratic intelligence flows, placing difficult demands on intelligence staff, and increasing the level of noise and interruption. Adversaries, both state and non-state, may recruit, indoctrinate, and train expert hackers and cyber specialists, and they will target U.S. Army and other U.S. services and assets. For example, U.S. cybersecurity firm Mandiant released a report identifying the Chinese People's Liberation Army (PLA), specifically Unit 61398, as the perpetrator of a huge number of aggressive cyberattacks. The report provides robust and comprehensive evidence to substantiate its deductions.[12]

The theft, subversion, and complication of data would reduce our ability to achieve a credible and

reliable "whole system" picture of both friendly and adversary activities, further increasing the effort required to achieve insight and to support decision-making. In these convoluted circumstances, planners and commanders must understand the important relationships between targets, audiences and adversaries, their environment, and neutral actors. The combination of the adversary, neutral actors, and allied forces will constitute a set of interconnected complex systems, themselves connected to, and part of, the overall environment.[13]

In summary, adversary intelligence functions and their C2 systems may be robust and unpredictable. It must also be recognized that an adversary could degrade allied information networks through a variety of means, to include physical sabotage, cyber methods, or misdirection.[14] As such, an understanding of the relevant indicators and warnings for the whole spectrum of threats is necessary to be able to make progress while uncertainty remains.[15] This will also facilitate the making of good decisions under difficult circumstances. However, an appreciation that what worked last time might not work next time is also necessary as well as an acceptance of unfamiliar and ill-defined risks.[16]

Unrestricted Adversaries

> The first rule of unrestricted warfare is that there are no rules.[17]

Present and future adversaries may not be bound by the same rules of engagement as the U.S. Army, other U.S. services, or their allies. Some of the U.S. Army's potential competitors are already committed

to aggressive information activities ranging from elementary but effective disinformation operations to the nuanced use of multiple channels. For example, ISIS produced propaganda material responding to President Donald Trump's ban on immigration from certain countries, claiming that Islam cannot be defeated. While President Trump has not asserted any intention to defeat Islam, the message remains potent because there is a willing audience.[18]

As diverse information channels and tools become cheaper and more readily available, terrorist groups will adopt some of the methods and systems that would previously have been exercised at a national level. For example, in addition to recruiting fighters from the global pool by use of carefully targeted multilingual information campaigns, ISIS exploits an effective propaganda machine within the territories it already controls.

> ISIS also runs a sophisticated operation within the caliphate to brainwash the population it rules. The group has set up 'media points' in the cities it controls to maximize the exposure of its propaganda to the public. Videos, audio files, and other promotional materials are available directly from the media points using USB flash drives and SIM cards.[19]

While the propaganda may not be entirely credible, and is likely to appear biased by its target audience, constant exposure can be an effective approach:

> a majority of people don't believe [ISIS propaganda], but that coupled with a lack of any other information will impact thinking and decision-making, . . . It's totalitarian politicking. You can really break down someone's ability to resist the state.[20]

Furthermore, as the territory under direct ISIS control has shrunk because of Coalition military efforts, ISIS has successfully stepped up its online activities inciting individuals to carry out acts of violence in European cities.

Exposure and bias reinforce the beliefs of the terrorist. The U.S. Army should not assume that telling the truth will persuade, as plausibility is not always an adversary objective.[21] Criminal and terrorist perspectives may be driven often by what they want to believe.[22] Terrorist groups are now able to assemble a large enough number of fighters to rival a nation's army.[23] This poses the risk that the U.S. Army may have to engage in large-scale conflicts at short notice, with ill-defined adversaries that use asymmetric methods, in difficult physical and informational environments. While such variety and lack of definition may reduce the effectiveness of the assembled adversaries to some degree, they remain able to reestablish relationships rapidly without the need for top-down coordination. They may never be as efficient as the U.S. Army, but they may be robust, unpredictable, and highly agile.

The Headline Challenges

Against a backdrop of proliferating communications technologies, complexity, and unregulated activities by many belligerent groups, the most urgent challenges that face the U.S. Army in the pursuit of information dominance may be seen to be the sheer amount of information available to the intelligence staff and the commander. This is normally augmented by the proliferation of devices such as mobile phones throughout the world, and the adversary's aggressive use of information, including the sabotage of allied media and narratives.

The Data Deluge

There is a huge amount of data accessible through secret intelligence, open source intelligence, and multimedia streams 24 hours a day, 365 days a year. This presents the intelligence analyst, commander, and decision-maker with the problem of identifying and extracting information that is urgent, important, relevant, and true from the vast bulk that is none of these. The U.S. Army Operating Concept states an important but sometimes overlooked principle:

> because of limitations associated with human cognition and because much of the information obtained in war is contradictory or false, more information will not equate to better understanding.[24]

Advances in managing "big data" will mitigate this risk.[25] For example, work undertaken by organizations such as Sandia, a subsidiary of Honeywell International, Inc., will help make sense of massive amounts of data.[26] Automatic feature extraction will assist the analyst and enable wide area surveillance, providing earlier warnings of threats and items of interest.[27] Such technologies also help discover denial and deception by identifying anomalous relationships. There will remain challenges when the data has deliberately been corrupted, for example, under conditions of an adversary's deception. Determining whether data is corrupted requires a high degree of analysis, with limitations on the rate that data can impact the decision-making processes. This is relevant to the U.S. Army because the adversary will exacerbate uncertainties in order to slow down the Army's intelligence processes.

The Proliferation of Intelligence, Surveillance, Target Acquisition, and Reconnaissance (ISTAR) and Related Technologies

Less than 20 years ago, mobile phones were relatively uncommon, and few phones had integrated cameras. Now, camera-equipped phones are ubiquitous, and there are massive networks of connected users sharing images, videos, and text in near real time, on a global scale. In addition, the automatic uploading of data from many connected devices, whether intended to be public or private, provides unfiltered access to this information for intelligence agencies seeking to exploit it.[28] This unregulated global network represents both a risk and an opportunity; it is a risk to allied covert activities and operational security (OPSEC), and an opportunity for allies to gain intelligence against certain threats, such as terrorists or belligerent nations.[29] The cost of entry to the global information community is now negligible, and many commercially available information systems could be used directly in, or adapted to be part of, unmanned covert ISTAR processes.[30] In addition, the trend toward miniaturization means the devices have become smaller and hence harder to find even if not deliberately concealed. Improved battery technologies have also resulted in more energy for a given size, meaning that there are increases in endurance and hence the potential for greater standoff ranges.[31] The use of mobile phones as remote recording and transmission devices is commonplace. Consequently, the U.S. Army may find it harder to achieve surprise by maneuver if, for example, photographs and videos of the U.S. Army are being instantaneously propagated ahead of them by covert or overt means.[32]

As is the case with all armed services, the U.S. Army will have been, and will continue to be, a target of infiltration.[33] Miniature cameras, transmitters, and data storage and recording devices may increasingly be used to pass large amounts of information in and out of U.S. Army and other related sites without the knowledge or control of security staff. Secret information that could enable terrorist acts may rapidly attract a cash value, and it is likely that U.S. Army counterintelligence capabilities will be tested to the limit.[34]

Unrestricted Information Warfare (IW)

In tandem with the proliferation of networking technologies, we might expect adversaries to suppress competing stories, communications, and data by jamming transmissions, or hacking and bringing down websites.[35] One example is TV5Monde, a French television network, which was brought down by hackers in April 2015 using seven points of entry believed to be operating from Russia.[36] Such attacks may be part of a campaign by Russia to test and hone their technical intelligence gathering techniques and cyber arsenal on relatively easy targets.[37] More highly developed cyber weapons could threaten the effectiveness of the conventional media, mass communication, and friendly military systems.

"Fake news," the latest fashionable term for disinformation, has achieved a high profile recently on many media channels. Projects and associated sites such as Fact Check and The Integrity Initiative provide essential exposures of information manipulation.[38] Using a combination of part truths, emphasis, selective exclusion, and falsehoods, belligerent nations and groups are able to use highly connected media

and attention-grabbing actions to push their stories to the top of the international agenda, using social media to spread lies, dissent, and fear, and manipulating the media and democratic processes.[39] For example, the Russian expansion into Ukraine and the annexation of Crimea are supported by concerted IW activities in the Baltic States. The Russian IW sequence was tested in the Ukraine and has proven to be effective.[40]

Other recent examples of concerted campaigns of disinformation/fake news in conjunction with cyber effects include the U.S. Presidential election in 2016 and the French Presidential election in 2017. In the case of the U.S. election, American intelligence agencies have concluded with "high confidence" that Russia acted covertly in the latter stages of the Presidential campaign to promote Donald J. Trump.[41] According to James Comey, former Director of the Federal Bureau of Investigation (FBI) and James Clapper, Director of National Intelligence, Russia launched cyberattacks on the election to denigrate Hillary Clinton.[42] With respect to the French 2017 election, a similar attack occurred whereby internal campaign documents, including emails and financial data, were taken in an effort to undermine Presidential candidate Emmanuel Macron. Shortly before the polls closed, nine gigabytes of hacked documents were released online by an anonymous user and disseminated with automated bots. Although the source of the attacks has not been publicly named by the French authorities, Russian involvement is suspected partly due to support for the opposing candidate Marine Le Pen, who supports a pro-Moscow foreign policy, as well as recent evidence of Russian involvement in targeting Macron's campaign through the use of phishing emails, malware, and fake domain names.[43]

The Russian campaign to expand on its western front is based on well-coordinated and structured IO, and it carefully controls and influences both traditional and social media.[44] Russia is repeatedly implicated in media manipulation and attempts at destabilization. In February 2016, *Der Spiegel* reported on how Moscow achieves its strategic communications effects through spreading numerous targeted lies in order to achieve the "boy who cried wolf" effect. The simultaneous release of multiple false versions of an event has the effect of blurring the lines between what is real and what is fabricated. In other words, rather than to attempt to beat its opponent in its battle for the truth, Russia simply sabotages the whole game. According to one European Union (EU) insider specialist interviewed by *Der Speigel*, "Russian propaganda does not put out one version of a story but many, and in doing so, it pollutes the realm of information. In the end, people no longer believe any version—including the one that's true."[45]

A further intention is to generate dissent and anger.[46] This is achieved partially through troll factories, where employees known as trolls write and post blog entries or comments for news and other websites with the aim of agitating members of the Russian opposition, or Western democracies in general such as the EU and the United States. For example, on September 11, 2014, trolls triggered alarms in the United States when hundreds of tweets reported an alleged chemical accident in a Louisiana factory. The coordinated campaign of false information originated from trolls based in St. Petersburg, Russia. However, the main concern was that it was likely to have been a test run for future, larger-scale disinformation campaigns originating from Russia.[47] The United Kingdom's (UK)

Telegraph also reports on the British Government's acknowledgement of the role and extent of Russian IW activities.[48] While some of the Russian IO appears almost comical in the West, the tight control over their own media ensures that the domestic Russian populace is regularly fed a conveniently pro-Putin information diet.[49]

While several nations and terrorist groups practice their influence across all communications channels, the protection and defense of military systems has not been put to one side. Nations and groups will continue to camouflage their weapons, intelligence, and communications system. For example, in the unclassified domain, rumors abound of North Korea's underground facilities.[50] Signature masking and signature adaptation, for example, of vehicles, bunkers, missile systems, and suicide bombers, could make it challenging to discriminate between real and decoy physical targets in congested and noisy environments, even with advanced sensors. In response, there are clear indications from industry that a holistic approach to information management should be adopted, and that technology alone is not a universal solution.[51]

It must also be assumed that adversaries have competent counter-deception capabilities. There is a risk that if the U.S. Army or its allies exploit simple deceptions, these actions may fail, and it will be easily outmaneuvered.[52] Of course, we should not expect to see much in the way of evidence of these failures, as adversaries will take all possible steps to make the United States believe deceptions have been successful.[53]

It follows that the U.S. Army should be prepared to field more robust and potentially complex deceptions in support of its strategic objectives—enough to overmatch the adversary's counter-deception capabilities.

The U.S. Army can use combinations of deceptions and other aggressive IO as force multipliers, reducing the adversary's effectiveness and confidence.[54] The exploitation of several mutually supporting IO is generally more effective than the implementation of elementary deceptions that are single-outcome strategies.[55]

U.S. doctrine states, "the key to a Strategic Win is to present the enemy with multiple dilemmas."[56] One way to achieve this is to offer complex and multiple deceptions to disrupt adversary planning and decision-making. In order to reduce cost and increase the cognitive load on the adversary, some simple deceptions can be launched in order to provide the appearance of more complex deceptions, increasing uncertainty in the adversary's mind, and perhaps helping obscure friendly intelligence actions.[57]

The U.S. Army and its adversaries will both try to make planning and decision-making more difficult for each other, exacerbating the challenges that complexity and deception can bring. Each operation launched by an actor is likely to affect several different parts of the target complex system and other connected complex systems. The planners and decision-makers who are adept at understanding the networked nature of targets will be able to make better decisions than those who assume independence between objects in the information and physical environments. Recognizing connectedness and complexity should be a routine activity for the analyst and the planner.[58]

Risks

Primary Command and Control (C2) Risks

The U.S. Army's C2 systems are likely to be one of the adversaries' priority targets.[59] We suggest some examples of risks that illustrate potential activities and outcomes, as follows:

- The operational level C2 structure might be targeted, with a large number of cyberattacks attempting to remove, alter, and insert commands, for example, by subverting error-checking codes.[60]
- The U.S. Army Operating Concept observes, "Information systems connect the strategic sustainment base to tactical organizations to anticipate needs and provide a high degree of responsiveness and reliability in the supply chain."[61]
- This makes information technology in the supply chain a primary target for adversaries, both in peacetime and in conflict. The risk is that the hardware and software within U.S. Army C2 systems could be degraded and manipulated.[62]
- The tempo of IW may increase to the point where the mean time between significant events is shorter than the time needed to generate rational decisions or resolve ambiguities. This will affect the U.S. Army, its allies, and its adversaries.
- The tempo of events, conflict, communications, and distractions might rise and fall unpredictably, placing difficult demands on the resourcing process.

- Adversaries may have mature deception strategies that are tested and versatile, and focused on U.S. Army assets and processes.
- Adversaries could corrupt, jam, and spoof U.S. Army tactical communications and insert messages and sounds that are intended to mislead, distract, and confuse Soldiers.[63]
- Adversaries might cause global positioning system blackouts, whiteouts, and noise, and they might try covertly to manipulate systems, perhaps by inserting false targets.
- Cyberattacks could increase uncertainty in command and intelligence systems, and adversaries could seek to reduce uncertainty falsely by reinforcing belief where there should be doubt.
- Adversaries might use swarm techniques in order to overwhelm U.S. Army intelligence systems and to clutter the operating picture.

Primary Defense Intelligence Risks

- There may be multiple targets and adversaries in the physical and informational environments, requiring more information than can be attained or understood in the time available.
- The intelligence analysis might fail to recognize unfamiliar threats, for example, if they are buried in bulk data.
- Adversary counterintelligence systems might prevent us from gaining the intelligence required to prosecute threats or defend our assets.
- Some threats might behave in an apparently irrational fashion, making it difficult for analysts to predict their behavior.

- Emerging technologies might provide incremental or game-changing advantages for adversaries.
- Adversaries and belligerents may feign actions, vulnerabilities, and provide false feedback in order to divert and manipulate allied intelligence activities.
- Intelligence systems could experience multiple cyberattacks simultaneously.
- Adversaries may feed bulk information to clog the intelligence channels and process.
- The adversary could use convincing physical camouflage and dummy systems that will challenge friendly detection and counter-deception methods. Given the proliferation of high technology sensors throughout the battlespace, and indeed land, sea, air, and space as a whole, the contest to spoof and conceal will escalate with complex deceptions. This introduces the concept of "signature warfare" and emphasizes the need for the U.S. Army to adopt and excel in this area.

Primary Information Warfare (IW) Risks

- Adversaries may feed credible false information into intelligence systems and processes in order to lead the U.S. Army to construct the wrong hypotheses, and to manipulate decision-making to the adversary's advantage.[64]
- Adversaries may have extensive intelligence and counterintelligence networks that are not constrained by any laws or any ethics, and that are unpredictable, meaning that the U.S. Army is outmaneuvered.

- Some adversary intelligence services are well-prepared, well-funded, and well-organized. It is sensible to assume that they will already have started their own advanced covert operations in several areas of potential conflict or competition.[65]
- U.S. Army supply chains may be targeted. The adversary may attack databases and, for example, may alter schedules in order to prevent the effective supply of munitions, food and water, spares, fuel, and medical goods.
- Uplink and downlink communications for drones might be jammed, spoofed, or manipulated by the adversary's cyber specialists to remove or insert items.[66]
- Adversaries may exploit their own highly protected special capabilities, including technologies and IO.
- Adversaries may engineer events to make it appear that third parties are involved in actions that they are not.

Summary

The U.S. Army is an attractive target for adversary commanders and fighters. It could experience diverse forms of attack, varying in scale, sophistication, and tempo. Its adversaries might range from nations practicing conventional and specialized warfare to small groups exploiting irregular forms of warfare. There are many risks to its C2 operations, and to its intelligence and IW capabilities. The challenges include: significant uncertainty; sudden unexpected events; high noise and clutter levels in intelligence pictures; basic

and complex deceptions through a variety of channels; the actions of hidden actors; and novel forms of attack on U.S. and allied command, control, communications, computers, information/intelligence, surveillance, targeting acquisition, and reconnaissance (C4ISTAR) systems.

The U.S. Army needs to maintain information dominance in all environments, but in order to achieve this, it must exploit the complexity and uncertainty in the battlespace and not simply seek to overcome it. While determination and commitment are necessary, they are not sufficient—to achieve and maintain information dominance, the U.S. Army will also require: a significant injection of innovation; a robust and resilient C2 and intelligence capability; novel technologies; and an accelerated IO capability development program that is broad, deep, sustained, and well-coordinated. The U.S. Army's prowess in conventional warfighting should be augmented by the exploitation of advanced special operations in the technological and informational domains, expertly and rapidly integrated, using tested multiple outcome strategies that will survive and succeed in uncertain and very aggressive circumstances.

PART 2: INTEGRATION

> To win in a complex world, Army forces must provide the Joint Force with multiple options, integrate the efforts of multiple partners, operate across multiple domains, and present our enemies and adversaries with multiple dilemmas.[67]

The U.S. Army is committed to a high state of resilience and readiness. The problem is that for complex environments, the U.S. Army cannot afford simply

to be very effective in a known set of circumstances and unprepared for others, and neither can it afford to be only moderately capable in the broadest possible range of circumstances. The U.S. Army has to be very effective across the board, in all phases. This means the U.S. Army must prepare a significant portfolio of IO material, procedures, and responses for use in information contests, and be well-trained in the rapid selection and integration of IRCs. The volume of material in this portfolio, and the potential combinations and sequences of operations, will place extraordinary demands on the integration staff and the integration process itself.

Structurally, the U.S. Army is central to joint operations. The U.S. Army provides multiple options in support of the Joint Force Commander's (JFC) objectives.

> Joint operations are critical to cope with such complexity, and the Army's contribution must provide unique capabilities and multiple options to the President, Secretary of Defense, and Combatant Commanders.[68]

The Joint Information Operations Warfare Center ensures the integration of all IRCs in support of IO, and at the international and coalition level, coordination is undertaken by Joint Staff.[69] This means that the integrated operations work together symbiotically to achieve the desired effect, enabling force multiplication and an effects-based approach.

> IRCs can be capabilities, techniques, or activities, but they do not necessarily have to be technology-based. Additionally, it is important to focus on the fact that IRCs may come from a wide variety of sources. Therefore, in IO, it is not the ownership of the capabilities and techniques that is important, but rather their integrated application in order to achieve a JFC's end state.[70]

One of the key benefits of integration is that it supports deconfliction. This ensures, for example, that messages to a target audience do not contradict each other, and that actions do not contradict messages. It can also reduce uncertainty by helping the right information flow through a complex organization.[71] It should be noted, however, that as previously highlighted, contradictory messaging is not a constraint for adversaries. In fact, conflicting messages can be used as a means of introducing confusion so that neither true nor false messages are believable to the audience.

Integration also plays a vital role in the intelligence function. Not only does it bring together the collection, analysis, and dissemination processes, but also it enables other operations to protect the intelligence capabilities and activities (for example, by misdirection, camouflage, deception, and distraction) and sometimes to enhance the intelligence process by stimulating the target to provide the information that we seek.[72] The expert coordination and synchronization of operations may simultaneously provide intelligence and deterrence via a number of channels, such as cyber, diplomatic, psychological operations, and deception. This can provide a strong basis for subsequent operations by de-risking specific courses of action and allowing more options for the commander to take later in the engagement.[73] This matters to the U.S. Army because it permits the commander to adapt his C2 and his intelligence activities to unfolding circumstances.

Integration enables several activities to be effective, including IO, military information support operations, intelligence, and strategic communications. All of these activities support the objectives of the commander by influencing many targets, including by

educating and informing populations and disrupting and exposing adversaries.[74]

Integrating multiple actions in a complex environment is a demanding and highly labor-intensive activity. The integration exercise is exacerbated by the fact that staff do not know beforehand how many or which adversaries they will need to neutralize, and they often cannot know exactly where there will be conflicts, how events may unfold, and which will be the commander's highest priority options or courses of actions.[75] We have seen how adversaries might attempt to corrupt the intelligence and integration functions by providing misinformation and noise; this makes integration even more of a challenge.

Although the U.S. Army and Joint Forces undertake extensive and rigorous training across multiple stakeholders, simulating a variety of scenarios and events, it remains likely that many capabilities will have to be integrated rapidly in unfamiliar, fast-changing, and potentially deceptive conditions. In order to retain agility and speed, a commander may decentralize some assets and permit them to operate within a specific operational envelope.[76] Such actions allow high-level integration, while delegating risk management to the appropriate level and giving latitude to make tactical and operational decisions quickly.

In a complex engagement, it is likely that multiple kinetic and IO must be seamlessly integrated. At the same time, the adversary may exploit multiple linked operations, targeting several actors in the contested space. The U.S. Army's IRCs must be able to address the challenges of the data deluge, the proliferation of ISTAR systems and hostile information manipulation, as well as other significant risks. This presents the U.S. Army with the simultaneous challenges of the

complexity of the environment and the rapid tempo of events.

The concept of overmatching applies not just to warfighting, but also to complex systems. For one system to dominate another, it must control that system (in the academic literature, a system is often said to be "regulating" rather than "controlling" another). In our context, we wish to control not just the adversary, but also the information environment, and hence the perceptions of the adversary and indeed neutral actors, who may have been deceived and influenced by the adversary.

Insight into the control of a complex system is gained by referring to Ashby's *Law of Requisite Variety*.[77] This "law" asserts that, in order to control a complex system, the controlling mechanism needs to have at least the same variety/complexity as the object to be controlled. The "controlling mechanism" is the U.S. Army and its allies. The "system" is the adversary and the environment. The "tasks" are the operations and actions that the U.S. Army undertakes; integration is the coordination of these tasks. This is articulated well by Ken Thomson, a consultant in team development:

> The law tells us that a 'system' only has 'requisite variety' if its repertoire of responses is at least as big as the number of different stimuli it may encounter in its environment. A system without requisite variety will fail whenever it encounters the unexpected and as such is not a 'viable system'.[78]

Put in these terms, for the U.S. Army to control a complex system that includes adversaries and a complex environment, it needs a greater variety of operations than the adversary, and enough options to account for any major eventuality that may arise in the

environment. This is an intuitive step, which implies a move away from reliance on intensity, namely conducting operations simply with more energy or speed, and instead toward an understanding of the requirement for several linked and mutually supporting activities that envelop the environment, and how to enable them. For example, inexperienced or naïve planners may treat a cyber threat as a purely technical problem, and this tends to elicit a technical response. In reality, the humans behind the technical threat may be launching other attacks in parallel.[79] An inability to grasp the actual complexity of an attack will lead to failure. This introduces the risk of the target being predictable and easily drawn into a series of pointless technical diversions while the real damage is being done elsewhere.[80]

When confronted with a task, adversary, or environment more complicated than one can currently manage, there are two options:

1. Increase the variety in the regulator (also known as amplification).
2. Reduce the variety in the system being regulated (also known as attenuation).

In fact, the U.S. Army could choose both options, and increase its available set of IO ("amplifying" the available variety), while using warfighting methods to "attenuate" the target. This could be by attrition—reducing the connectivity of the system and the available options for the adversary commander. This is a method of dealing with the complexity of the environment, as well as with the adversary. Examples of how to increase the variety of operations are provided later.

In order to address the challenge of high-tempo operations, the burden on the integration staff and the commander must be reduced as much as possible so

that they are able to make faster and better decisions. In addition to the provision of tools to address complexity, we can prepare the Force by analyzing operations and their use, risks, dependencies on other operations or circumstances, support they can offer to courses of action, and likely outcomes and potential scenarios. This preparation of operations and corresponding analyses is likely to present the integration staff with more combinations of operations, allowing them to select from a wider portfolio of actions and capabilities, and benefiting from a head start based on the early analysis. With this variety, the commander can overmatch the adversary and control the environment.

The task of integrating operations, synchronizing and coordinating from the tactical up to the strategic level, across all phases of warfare is immense, and integration is the fulcrum. If there is an inadequate variety of tools for the commander, or the integration is ineffective, the U.S. Army will struggle to achieve parity with an unconstrained adversary. With innovation, preparation, and robust integration, the U.S. Army can achieve information supremacy. Integration is the means by which the IO, and all other operations, work together to achieve the control that is required for information dominance.

PART 3: SOLUTIONS

Because of the variety of risks and opportunities in a complex environment, no single action or venture will sustain information dominance. In order to achieve and maintain dominance, the commander must have access to a wide variety of innovative IO that can be seamlessly integrated with the Joint Plan, be confident that his C2 and intelligence systems are

resilient to attack and subversion, and rely on well-trained staff. This, coupled with the use or threat of overwhelming force, is a good start.

In this section, some potential solutions are outlined by revisiting the headline challenges.

Data Deluge

The data deluge is both a risk and an opportunity for the U.S. Army and for its adversaries. To achieve dominance, the U.S. Army must make the most of the opportunities presented by having access to massive amounts of data, while ensuring that the adversary cannot operate effectively, for example, by making it also difficult for the adversary to select relevant data from the bulk. Similarly, the adversary may seek to achieve advantage by overloading the U.S. Army's intelligence and C2 functions.

Therefore, the U.S. Army needs to exploit advances in data management, selection, pattern matching, and hypothesis generation by working with academia and industry, as well as continuing to share concepts and research, for example, through existing international technical cooperation programs with partner nations.[81]

The application of advanced hardware and software to massive data problems should be complemented by investing in intelligence analysis by humans; one route is to provide a sustained and advantageous career path for promising individuals, ensuring the profession is recognized as applicable to many real world opportunities within the defense, intelligence, and security communities and in wider business.

One of the components of intelligence analysis that should be developed further is counter-deception. Deception and other forms of manipulation

may be used by the adversary and the U.S. Army in many ways. For example, they may provide false but attractive information in bulk data, provide overwhelming ambiguity, divert the adversary's intelligence collection efforts, and reduce an adversary's confidence in the truth. They may even increase the adversary's confidence in falsehoods, and even appear to undertake these manipulations when, in fact, there is no actual operation (this is explored later in the topic "sublime operations"). The intelligence expert has to account for very many possibilities, including deception, without spending all his or her time on imaginary threats and tactics. He or she is simultaneously under pressure to produce intelligence summaries rapidly, without the time fully to resolve, analyze, or discard all potential hypotheses. It is a complex task, and participation is worthy of investment and recognition.

Given that all actors experience the same problems of bulk data, ambiguity, and the potential of deception and forms of information sabotage, the U.S. Army should take every opportunity to exacerbate the adversary's intelligence challenges. In addition to developing and recognizing the contribution of intelligence staff, the U.S. Army should field a strong tactical and operational level active counterintelligence capability that deliberately targets adversary intelligence functions and undertakes various activities to mislead and degrade them. It is vital that there is proper coordination between allied intelligence staff and allied counterintelligence staff; otherwise, there is a risk that they will inadvertently work against each other. This essential integration activity will extend to synchronizing kinetic operations, and the use of physical deception measures to support aggressive counterintelligence ventures. There is common ground between military

deception and active counterintelligence activities, and staff must work together for a common purpose when there is shared responsibility for an action. Clearly, the integration cell has a pivotal role in these activities at every stage, including cueing intelligence assets to verify outcomes, coordinating decoy activities, and preparing to deploy counterintelligence actions.

Proliferation of ISTAR and Related Technologies

The information environment may contain multiple ISTAR systems operated or exploited by adversaries, and indeed many surveillance systems that supply legitimate media organizations. In order to control the information environment, the U.S. Army may choose to destroy threat information systems, exploit them, or ignore them. Some destructive systems can operate over a wide area and can be used to "sweep" threat sensors without each one having to be isolated separately. Electronic warfare can be used to jam a network of sensors, destroy the systems themselves, or exploit them to spoof the adversary. Technologies in the field are advancing, and the need to coordinate many capabilities is critical. The U.S. Army has developed tools to control and enhance electronic warfare capabilities.[82]

The U.S. Army may also decide to exploit the adversary's ISTAR systems (and neutral information systems, such as media and reporting agencies), feeding in suitable data in order to manipulate the perceptions and hence decision-making functions of the adversary commander. This action requires coordination. Special Forces, for example, might be tasked to identify and manipulate several ISTAR systems in a contested area to distract the adversary's intelligence staff from other operations undertaken by the U.S. Army

nearby. Special Forces might encourage the adversary to believe that there is a distraction underway in order to increase their level of confusion—another example of a sublime operation. Repeated manipulations of sensors can be used as a conditioning activity to permit a real operation to be launched at a time and place of the U.S. Army's choice. While it may be hard initially to gauge the effect of such operations, if they are well-integrated, they can be used to help protect intelligence gathering, confuse the adversary's defensive measures, encourage the adversary to employ the wrong weapons, monitor the wrong locations and communications, and use inappropriate tactics in an engagement. U.S. Army Soldiers should be encouraged to understand the value of aggressive IO so that they can play an active part when they are tasked. This awareness, coupled with rigorous counter-deception analyses and innovative disruptive capabilities, will support the U.S. Army's imperative to achieve information supremacy.

Adversary Information Warfare (IW) and Kinetic Attack

The U.S. Army and its adversaries face the challenges of complexity, uncertainty, and time pressure. Some adversaries will be patient and clever, and others will be impetuous and irrational. There is no one defensive measure that will protect the U.S. Army's C2 and Soldiers from attack. However, as with the conceptual solutions for data and ISTAR systems, a coordinated defense offers an effective basis for a powerful offense.

The U.S. Army should have reliable counter-deception capabilities that overmatch the adversary's deceptions. This will require rigorous training, competitions, exercises, and research into potential deceptive

methods used in modern warfare. Counter-deception staff will require substantial patience as well as excellent analytic skills. These staff will need to work with the planning cell to develop and implement means to outmaneuver the adversary. It is no longer a reasonable strategy to insist on there being clear evidence of a deception's existence before acting to counter the potential implications of a putative deception. Any competent adversary will mask the evidence of that deception and probably fabricate evidence to show that the deception does not exist.[83] The important principle that "absence of evidence is not evidence of absence" holds well here.[84]

Counter-deception staff are well-positioned to cue intelligence activities to help uncover deceptions, and to develop deceptions themselves. Any deception considered by U.S. Army staff must be passed through the U.S. Army's integration staff, as they will be aware of any other operations being undertaken (this is especially important with covert operations, where very few people have a need to know). The integration staff will be able to take the appropriate steps to ensure there is force multiplication, while minimizing the risk to friendly forces and staff.

In order to combat and neutralize adversary IW activities, the planner, deception, counter-deception, and intelligence staff must work together to ensure that they can control the responses of the adversary to the actions that the commander takes. The commander should be briefed on the sophistication of the adversary's operations, so that he or she can understand how to use resources to overmatch them with minimum wastage. In a complex and deceptive environment, we may never know if we have overestimated the adversary (and have expended far too

many resources defeating them), or whether we have accurately assessed their degree of sophistication (and have achieved success economically). It is only when an adversary outmaneuvers us, because we underestimated them, that the extent of any error on our part may become clear. By then, it is too late. This matters to the U.S. Army because it cannot afford constantly to proceed too cautiously, perceiving potential threats where there are none and deploying complex operations that massively overmatch an adversary. There is no analytic or technological solution to this, but experience and intelligence provide the insight that allows a commander to select the appropriate course of action.

The adversary will attack U.S. Army information systems using kinetic methods as well as deception, including potentially advanced technical sabotage. To achieve resilience under these conditions, C2 systems must exhibit graceful degradation (the ability to continue to function when degraded or damaged). The U.S. Army's technical defenses such as firewalls, operating procedures, and other OPSEC activities can be augmented by deploying sacrificial systems. If the U.S. Army deploys decoy C2 systems that can be detected by the adversary, then these are likely to attract the adversary's attention. They can be configured to provide the feedback the adversary will seek. For example, a combination of effects such as lights going off, radio silence, or changes in communications content. This will lead the adversary to believe that the U.S. Army's C2 function has been successfully disrupted, when in fact it has not. It is possible to deploy several of these sacrificial decoys in order to waste the adversary's time and gain intelligence on their methods and capabilities.

The adversary will manage, at some point, to degrade the U.S. Army's C2 and information systems.[85] The U.S. Army should continue to prepare for this by training for operations without access to friendly systems such as communications facilities or navigation equipment. It is possible that veteran staff will be able to describe situations and workarounds.

Training under these conditions will help Soldiers learn to survive complex attacks and will expose major vulnerabilities, allowing them to be strengthened. The exercises can then be repeated, testing the new defenses and new ways of working. These exercises could be designed and observed by selected experts from academia and industry.[86] Training under conditions of limited functionality is a valuable risk reduction activity and will refresh training regimes, challenging the trainers as well as the trainees. For example, one such competition could be arranged by having two units attempt to secure a position, where one unit has no navigation systems and the other has no communications systems. While the communications systems might prove more valuable in this engagement, it would be interesting to see how each unit developed workarounds. Each unit would want to increase their performance, and would inevitably try to develop strategies that make their opponents fail. In addition to the loss of some information systems, other forms of degradation, such as gaps in information traffic, would probably be experienced in conflict.

The adversary's attacks on the U.S. Army's decoy systems can be used as a weapon against them. A well-coordinated deception that indicates to the adversary that there is a failure of C2 can lure the adversary into a false sense of security and a false sense of advantage. At an appropriate moment, the U.S. Army commander may choose to reveal to the adversary that

the systems that were under attack are fully functioning—this might have just the demoralizing effect that is required. It will also reduce the adversary's confidence in its other forms of attack. This provides a benefit to the U.S. Army because it attacks the adversary's will to fight. A terrorist leader, for example, who realizes he has been attacking a patient, clever, and almost invulnerable target will be more susceptible to other of the U.S. Army's influences, as he will feel and appear impotent and foolish.

The U.S. Army can also take steps to control the tempo of the information contest, and perhaps therefore the physical conflict. By providing false intelligence to an adversary at an increasing rate, the U.S. Army can examine the response of the adversary, exhaust the adversary's intelligence resources and the condition of its staff, induce fatigue, and reduce the adversary's ability to concentrate. The U.S. Army can also choose to indicate a slowing down of events, when in fact it may be preparing for a rapid assault. To control the adversary's perceptions, overt and covert channels can be used, providing an overwhelmingly compelling narrative to the adversary. This applies to situations where we want the adversary to believe a particular idea, or when we choose to make him uncertain. The coordination of physical operations and IO is vital to achieving success.

Preparation

The prerequisite for undertaking such special IO is that the operational concepts are available at the point of need, and that they have been risk analyzed, described in depth, and subjected to tests and exercises where possible, so that the commander can be confident in their use. It remains for the integration

staff to position the operations properly; in sequence; updated and tuned to account for the latest and best intelligence; and arranged to exploit resources, the information environment, and the known or suspected susceptibilities and biases of the target.

Special Information Operations (SIO)

This monograph has referenced several opportunities for deception and active counterintelligence. These operations, and other sensitive, covert, or unusual specialist operations, are often identified as special information operations (SIO). SIO, used in concert with other special capabilities (including special technical operations, [STO]), can be valuable enablers and protection mechanisms for conventional operations.

The U.S. Army's use of SIO is an important component of its future asymmetric warfare capability. In addition to excellence in warfighting, the U.S. Army needs to be able to field a wide variety of IO to secure the advantage, and grow and exploit confusion in the adversary's mind. This is achieved by diverting, confusing, demoralizing, or disrupting the adversary's perceptions, decision-making ability, and their plans. This is important because it means that the risk to U.S. Soldiers can be reduced, and the Soldiers can achieve more if their adversaries are uninformed or misled. Proficient use of SIO will create cumulative effects, where each operation magnifies the effect of those already undertaken, and prepares the ground for subsequent operations. SIO are particularly useful when the commander wishes to put the adversary on the back foot, and, as such, they are one of the principal means by which the U.S. Army can achieve and maintain information dominance.

Again, this underlines the vital importance of the integration cell—they have to coordinate SIO, mainstream IO, and conventional warfighting measures in order to achieve protection of their Soldiers, as they advance into uncertain territories.

The Operational Collection—an Information Operations (IO) Playbook

It has been noted that the U.S. Army commander will benefit from being able to select IO, including SIO, from a collection (or playbook). The chosen operations could then be modified to fit the prevailing circumstances, the characteristics of the environment, the target, and the (Joint) plan though the usual integration process.

The provision of such a collection will require concentrated innovation, analysis, competitive exercises, and rigorous selection procedures, driven by experienced military staff and subject matter experts, and supplied by a diverse community from academia, industry, and a range of social backgrounds. Once prepared, the collection of operations could provide significantly more options for the commander than available at present. This is relevant because without a collection of pre-analyzed operations to consult, the commander will have the choice of either developing and analyzing IO from scratch or proceeding without the options altogether and relying solely on kinetic capabilities—perhaps placing Soldiers at risk and reducing potential options later in the engagement.

Information Operations (IO) Playbook—Preparation

The preparation of such a playbook would be labor-intensive. Ideally, this work should be undertaken in times of relative peace to permit reflection, and uninterrupted and concentrated study by relevant staff and communities. Working in peacetime is not just easier, it reduces the work that has to be undertaken at the time of conflict when resources tend to be scarcer. This matters to the U.S. Army because during times of conflict it will free the commander and his or her staff to concentrate exclusively on the actions and orders that must be addressed at that time.

The preparatory stage can be undertaken in a cyclic fashion, starting with work that requires innovation. A model for undertaking this capability development could include the formation of several working groups, as follows:

1. Innovation Group—this should be drawn from a wide range of academic and industrial backgrounds, allowing technologists, inventors, designers, entrepreneurs, social scientists, historians, cultural experts, psychologists, and others to contribute. This group should be tasked to consider what operations could be used to overcome certain problems, counter hostile operations, or provide certain effects.
2. Scenario Staff—innovators from the Innovation Group will require context that helps them understand the problem, such as adversary actions, target information (including, for example, populations, neutral actors, and adversaries), and realistic examples of congested and highly contested information environments. These target and environment descriptions will provide use-

ful opportunities and constraints, and experienced IO staff can ensure the ideas and analyses are realistic and focused, using a series of "what if" scenarios in competitions between operational concepts, played out in a series of organized contests. Scenario staff could supply all this contextual information.

3. Red Team—this team should realistically reflect the methods and practice of nations and terrorist groups. The team could undertake research that shows what activities, tactics, and technologies may be used against the U.S. Army. Some adversaries may be very clever, well-funded, unconstrained by ethical and legal constraints, and with special capabilities of their own. Other adversaries may be unpredictable, irrational, and impetuous. The formation of this team provides another opportunity to exploit contributions from a wide community. The U.S. Army can also bring in staff from, for example, the Central Intelligence Agency and the National Security Agency to ensure breadth and depth and to invite a comprehensive challenge to the nascent operations.
4. Analysis Group—this should record, analyze, and compare activities, effects, risks, and opportunities during the research and competition stages, and then collate and summarize this material. The risk analysis may constitute the bulk of the preparatory work. It will require experience, insight, and a thorough assembly of relevant risks, indexed so that innovators and military staff can interrogate the database and understand what risks are contained or introduced, what effects can be achieved, and what

> methods there are to protect or enhance other influence activities. This enables rapid and effective integration at the point of use. The analysis will explore potential sequences, measures of effectiveness, effects, potential failure modes, and second order effects. Some operations will work well together and will provide mutual protection, such as, some intelligence and some distraction actions. Others may conflict, such as destroying adversary communications infrastructure, and inserting false information into their C2 operating picture. The preparation will identify coordination and synchronization issues for the operations, and for groups and sequences of operations.

At the first iteration, these groups collectively could generate, analyze, and select the initial collection of operations. For the subsequent iterations, the initial collection of operations could be developed during further competitions, as well as through analysis and particularly from use during conflict. The Analysis Group can refresh the concepts and pass the enhanced operations back to the Innovation Group, with a challenge to improve them, or indeed to counter them. The Innovation Group's countering of these operations will supply the Red Team with material to use, and the Innovation Group can then be challenged to counter them in turn. This design spiral will allow variations on many basic operations to be explored and subsequently exploited. In particular, the best material can be added to the playbook and offered to military judgment panels for exploitation by the U.S. Army. In this way, the U.S. Army can explore ways that its adversaries might work against it, and synchronization and

coordination issues can be recorded to allow rapid and effective integration in times of conflict.

The series of structured challenges would test ideas and assumptions, and pit teams with different approaches against each other, providing a safe environment to explore new techniques against deceptive opponents, and opponents with unknown perspectives. The competitive nature of the exercises is key to success. It is essential that these competitions are monitored to see what strategies are effective and for how long. This will present valuable training material for intelligence and the integration staff.

Experienced military staff (including veterans), and civilian subject matter experts can observe and influence the innovations, analyses, and competitions, helping prioritize and select the most promising concepts for inclusion in the overall collection. It is important that the commander, at some point in the future, knows that the ideas have been judged militarily viable by suitable staff.

Examples of Special Information Operations (SIO)

The examples of SIO given here and many others can be developed in support of other warfighting operations in order to reduce risk and provide options. They do not generally replace any existing activities or capabilities but provide ways to exploit the complexity and uncertainties in the information environment by being deployed alongside other operations, enhancing their effect, and providing protection and diversion.

- Perturbation—the U.S. Army can undertake operations that perturb or stimulate a target so that it reacts in a way that supports the U.S. Army's intelligence activities, including

detecting the presence of the adversary's clandestine assets. Perturbation can be used as part of a wider endeavor to degrade adversary intelligence agencies and exhaust their intelligence channels.

- Signature Warfare—the U.S. Army will often be the first forces on the ground and will advance through urban and open landscapes at a relatively fast pace. It follows that the U.S. Army should have expertise in controlling the visual, electromagnetic, and other signatures given off by their vehicles, Soldiers, communications systems, electronic warfare (EW) platforms, special capabilities, and decoys. The U.S. Army should be able to forward-deploy jamming devices, false targets, false capabilities, and programmable signature generators in order to defeat the adversary's defense, target acquisition, and maneuver strategies. This coordinated activity might be termed "signature warfare." It is an area in which the U.S. Army can take the lead. It is related to military deception and to active counterintelligence and can support the OPSEC objectives.
- Emergency Intervention—these are interventions that can cause delays, buy time, disrupt high-impact threats, divert, or otherwise disrupt. They include actions such as dazzling, swamping, overwhelming, or simply confusing adversary intelligence functions that threaten to achieve high-value intelligence against us. They can be used, for example, to reduce a high-impact risk to a medium-impact risk.
- Conditioning—these activities consist of repeated actions or events that may initially be

of interest to the adversary, but appear after time to become less interesting and more usual. They can be used to make the first stage of an attack appear relatively non-threatening by repeating it and encouraging the adversary to associate it with benign circumstances. False conditioning leads the adversary to think you are conditioning them and keeping them alert. This can be used as a decoy or a sublime operation.

- Intelligence Protection—intelligence activities and signatures can be protected by providing false evidence of movement, infiltration, and the manipulation of adversary communications to indicate that one of their systems is being compromised, in order to draw their attention away from a genuine intelligence operation. Such operations must be fully integrated, as there is a risk that they may inadvertently expose other intelligence activities. Protection can take the form of conditioning, whereby a target is repeatedly shown some information or a series of events, so that they cease to take any strong interest. Protection requires planning and is effective when coordinated with other SIO.
- Open Operation—this category describes activities that use information items that can be deployed at an early stage and used later to reinforce, support, develop, counter, or adapt the narrative of our choosing. At the time of deployment, its purpose or intended outcome is not defined, but such operations can be adapted later by being coupled or associated with another activity, providing a means by which the emerging requirements of the commander can be achieved. An example is to fly a drone

over an enemy position. At this time, there is no particular purpose other than to prepare for a requirement that may emerge later. Should a requirement arise, the intelligence staff could, for example, purposefully permit adversary intelligence staff to intercept a message, indicating that the drone has gained some valuable target data such as the position of adversary tanks. This could be used to provide cover for allied human intelligence (HUMINT) sources, who would have supplied the real intelligence about the tanks to the U.S. intelligence staff, and the HUMINT sources would have been at risk of exposure had the tanks been targeted without another plausible explanation being available to the adversary's security and counterintelligence staff. While this may appear somewhat convoluted, these actions are realistic and viable for the U.S. Army but supremely difficult for the adversary to identify and counter.

- Sublime Operations—this type of operation consists only of the appearance of an operation. Sublime operations can be exploited on their own in order to disrupt normal processes, or concurrently with other more complex operations, acting as a force multiplier or supporting activity. They are generally low cost and low risk, and are useful when the commander wishes to increase uncertainty in the adversary's mind.
- Bulk Feed—this activity may be used to disable an adversary intelligence channel by providing a large amount of information that looks promising, but is generally useless. The process may or may not be covert, and could be used as a diversion or to mask another activity.

- False Capabilities—this function can be exploited to disrupt, demoralize, or divert targets; or to act as decoys or distractions. False capabilities may be used in conjunction with other confusing or compelling actions to provide protection, as they can be used to draw attention away from sensitive (real) capabilities. Alternatively, this can be exploited simply because it is disruptive. False capabilities align well with open operations and sublime operations.
- Active Counterintelligence—this is the deliberate process of manipulating a target intelligence system to meet military objectives. It may be used in all phases. Active counterintelligence can exploit a variety of simultaneous operations to support friendly intelligence operations, military deception, counter-deception operations, and non-military functions such as diplomatic and economic enterprises. It is very effective against both terrorist groups and nation states. A well-designed operation uses the characteristics of the target against it. It can, for example, provide the information that the target seeks, or that will reduce the target's confidence in genuine intelligence. The operations can be run concurrently or serially, and with mutual consolidation, meaning that every bit of information that is passed to the target intelligence channel reinforces the hypothesis we wish the target to have, or reinforces the uncertainty in their own staff, channels, human intelligence and technical intelligence. Active counterintelligence works well with other SIO, and can be a vital part of force protection, for example, by helping confirm in the enemy leader's mind an idea that the

U.S. Army would like him to have, or indeed to disincline him from believing an idea that we do not want him to believe.

SIO Summary

These examples represent some of the many types of available SIO and variations to these can be developed, analyzed, and recorded. If the analysis is adequately rigorous, then the operations' designs can be made available as specific planning options, for example, to divert a threat, to contain a risk, to delay the onset of an event, or to mask another activity. There are several operational designs that simply reduce the effectiveness of hostile intelligence activities, and have no other effect. Although it might be hard directly to measure the effect of these degrading operations, there is low cost and risk to the U.S. Army, so they should be considered. The development of a comprehensive set of innovative and thoroughly analyzed procedures will support the U.S. Army's commitment to readiness.

Organizational Measures

Much of the investment required to achieve the capabilities outlined in this monograph involves training and preparation of material using resources from the wider domestic and international community.[87]

Doctrine

Existing doctrine includes comprehensive guidance on the planning and implementation of IO, psychological operations, and special operations. There may be an opportunity to emphasize the value of

using a variety of SIO in the intelligence preparation of the battlefield (IPB) activities, in order to reduce the adversary's IPB activities.

Organization

At the organizational level, existing IO staff may need to be augmented to include some new posts. There will be additional educational demands, and there may be a need to work very closely with a variety of civilians in order to produce the innovations required for information dominance. There will be a need for mentoring to help develop specialisms, and it is recommended that IO specialists have clearly defined career paths to ensure that the staff and the U.S. Army all benefit fully from the investment in training and experience.

Training

There will be a need to train and test staff to fulfill the various specialist roles outlined in this monograph. Training would be a mixture of classroom, experiment, competitions, and highly focused self and group study.

Training topics should include deception, counter-deception intelligence, defensive counterintelligence (or OPSEC), active counterintelligence, rapid and deep integration, and a variety of SIO and counter-SIO. The integration function is the most critical—and it is here that a coalition of experienced Soldiers and analysts from different backgrounds can provide the feedback that is necessary to cover all the risks, opportunities, and combinations of circumstances.

Materiel

Existing intelligence and other systems may be used for SIO purposes as well as for conventional purposes. There will be a need to use existing educational facilities intensively for seminars, competitions, and analysis syndicates.

Leadership

In order to manage successfully the wider communities involved in the innovation and analysis stages, there will be a need for leadership that is firmly focused, but open minded. Retired military and civilian defense leaders might fulfill these criteria.

Personnel

Existing staff will be well-placed to become experts at information dominance and particularly active measures counterintelligence. There may be a need to recruit deep specialists. It has been noted that the need to operate in a complex environment at high tempo places a significant burden on the integration cell, so there may be a requirement to increase the complement of the integration staff.

During conflict and international exercises, staff may benefit from a permanent "reachback" cadre who can offer targeted and rapid deep research to support decision-making and options analysis. Such a cadre should be cross-disciplinary, with single subject matter experts and experienced military staff (for example, veterans) to mentor them.

The innovation, analysis, and competition cycle will require the participation of staff from outside the Department of Defense (DoD).

Facilities

There are no significant facility demands, but the training burden will increase so there may need to be a specific IO school made available, possibly outside DoD grounds.

Policy

There may be a need for some policy developments to help structure the use of the relevant capabilities. In particular, there needs to be a policy to cover the manipulation of intelligence and the rapid prosecution of terrorist groups using overwhelming information attacks. Special operations and active counterintelligence should be authorized, recorded, and controlled in a coherent fashion, according to proper policy.

Policy should enable the use of aggressive IO to reduce the risk to Soldiers and civilians.

PART 4: CONCLUSIONS AND RECOMMENDATIONS

Conclusions

The U.S. Army's adversaries will exploit all available methods to hinder, degrade, and destroy the U.S. Army's staff and capabilities, and will use asymmetric methods throughout all phases. Because the U.S. Army has to be highly effective in a wide range of circumstances, it must be prepared to defend its information systems against diverse information and physical attacks, while exhibiting graceful degradation. The U.S. Army staff must be capable of operating at near optimum levels without the full suite of defensive,

offensive, and communications systems; this means that it must train accordingly, including in joint exercises. The U.S. Army should also be able to deploy advanced special IRCs in support of its objectives, and overwhelm the adversary's intelligence and decision-making functions.

Integration staff are pivotal in the process of coordinating the significant existing conventional warfighting and information capabilities along with special capabilities. The tempo of events and speed of advance means that this integration represents an unprecedented challenge, so it must be supported by preparation and early analysis. This preparation and analysis will require the participation of a broad community, enabling the delivery of tested, robust, and versatile effects-based capabilities.

This may require that the U.S. Army staff develop new specialisms and career paths, providing continuous development for IO staff and further rewarding excellence in strategic and special IO professions.

Recommendations

In order for the U.S. Army, and more broadly the DoD and the Department of State to develop capabilities that enable information dominance to be achieved and maintained, the authors suggest that the U.S. Army implement the following recommendations.

Recommendation 1:

Develop and maintain a risk register that shows the priority IO risks, including the risks that IO might be able to mitigate. Use this register as the agenda for competitive innovations.

Recommendation 2:

Develop a process of iterative innovation and analysis in order to provide an extensive portfolio of effects-based operations that can be integrated rapidly to the Joint Plan (including during high-tempo engagements) with the minimum load and risk to the integration process. This will provide the commander with options to maintain information dominance.

Recommendation 3:

Train staff in complex and multiple deceptions; active measures counterintelligence; rapid integration; counter SIO techniques, including full-spectrum signature warfare using research, competitions, trials, exercises, and collaboration with trusted partner nations.

Recommendation 4:

Develop reliable counter-deception capabilities that overmatch the adversary's deceptions.

Recommendation 5:

Apply decoys, redundancy, deception, reversionary modes, and resilient technologies to ensure a sustainable C2 structure that can resist kinetic and information attacks.

Recommendation 6:

Exploit advances in data management, selection, pattern matching, and hypothesis generation by working with academia and industry, as well as continuing to share concepts and research with partner nations.

Recommendation 7:

Undertake competitive exercises using red teams to attempt to penetrate and (under controlled circumstances) sabotage the U.S. Army's own C2 and intelligence organizations and systems to identify and mitigate the vulnerabilities. Red teams should use all the innovative and alien concepts at their disposal.

Recommendation 8:

Encourage Soldiers to understand the value of aggressive IO so that they can play an active part when they are tasked by their own side, or targeted for exploitation by an adversary.

ENDNOTES

1. Headquarters, Department of the Army, *Information Operations*, Field Manual 100-6, Washington, DC: U.S. Government Printing Office, August 1996, pp. 1-9, hereafter, Field Manual 100-6.

2. M. Libicki, National Defense University Strategic Forum, No. 132, November 1997, p. 1.

3. Joint Chiefs of Staff, *Electronic Warfare*, Joint Publication 3-13, Washington, DC: Joint Doctrine for Command and Control Warfare, 1996, incorp. Change 1, November 20, 2014, p. v, hereafter, Joint Publication 3-13.

4. Keir Giles, "The Next Phase of Russian Information Warfare," Riga, Latvia: NATO Strategic Communications Centre of Excellence, 2016, p. 13, available from *http://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles*, accessed May 2, 2017.

5. Paul Mozur and Choe Sang-Hun, "North Korea's Rising Ambition Seen in Bid to Breach Global Banks," *The New York Times*, March 25, 2017, available from *https://www.nytimes.com/2017/03/25/technology/north-korea-hackers-global-banks.html?_r=0*, accessed May 11, 2017.

6. Joey Cheng, "DARPA renews efforts to deal with a crowded, contested spectrum," Defense Systems, April 28, 2014, available from *http://www.defensesystems.com/articles/2014/04/28/darpa-radiomap-ssparc.aspx?m=2,* accessed January 19, 2017.

7. Jane Wakefield, "How does IS communicate securely?" BBC, November 17, 2015, available from *http://www.bbc.co.uk/news/technology-34842854,* accessed November 19, 2017.

8. Robin Wright, "How the Arab Spring Became the Arab Cataclysm," *The New Yorker*, December 15, 2015.

9. Joint Chiefs of Staff, *The National Military Strategy of the United States of America,* Washington, DC: Joint Chiefs of Staff, June 2015, p. 1.

10. Lieutenant Colonel David C. Grohoski, Steven M. Seybert (Major, U.S. Army, Retired), and Marc J. Romanych (Major, U.S. Army, Retired), "Measures of Effectiveness in the Information Environment," *Military Intelligence Professional Bulletin*, Vol. 29, No. 3, January-September 2003, pp. 12-16.

11. James R. Gosler, "Counterintelligence—Too Narrowly Practiced," in Jennifer E. Sims and Burton Gerber, eds., *Vaults, Mirrors and Masks: Rediscovering U.S. Counterintelligence*, Washington, DC: Georgetown University Press, 2009, p. 177.

12. See Mandiant Consulting, "APT1: Exposing One of China's Cyber Espionage Units," 2013, available from *http://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf,* accessed March 9, 2017.

13. James Moffat, *Complexity Theory and Network Centric Warfare*, Washington, DC: Department of Defense Command and Control Research Program, 2003, p. xiii.

14. Giles, "The Next Phase of Russian Information Warfare," p. 3.

15. Gosler, "Counterintelligence—Too Narrowly Practiced," p. 177.

16. Moffat, *Complexity Theory and Network Centric Warfare*, pp. xii, 2.

17. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, Beijing, China: PLA Literature and Arts Publishing House, 1999.

18. An example of this anti-U.S. propaganda can be found at the following, Heavy Terror Watch, "ISIS Responds to Donald Trump 'Muslim Ban' Executive Order [PHOTOS]," Heavy, January 28, 2017, archived page available from *https://web.archive.org/web/20170608074623/https://heavy.com/news/2017/01/isis-islamic-state-donald-trump-muslim-ban-executive-order-immigration-islam-muslim-countries-terrorism-propaganda/,* accessed on August 9, 2018.

19. Pamela Engel, "It's Similar to North Korea': Inside ISIS's Sophisticated Strategy to Brainwash People in the 'Caliphate'," *Business Insider UK*, November 28, 2015, available from *https://www.businessinsider.com/isis-propaganda-strategy-2015-11*, accessed on January 3, 2017.

20. Ibid.

21. Keir Giles, "Handbook of Russian Information Warfare," NATO Fellowship Monograph, Research Division, Rome, Italy: NATO Defence College, November 2016, available from *http://www.ndc.nato.int/news/news.php?icode=995*, accessed May 25, 2017.

22. Brynjar Lia, "Al-Qaida's Appeal: Understanding its Unique Selling Points," 2008, available from *http://www.terrorismanalysts.com/pt/index.php/pot/article/view/44/html*, accessed on January 5, 2017.

23. Ahmed Rashid, *Descent into Chaos,* London, UK: Penguin, 2008, p. 17.

24. Training and Doctrine Command (TRADOC), U.S. Department of the Army, *The U.S. Army Operating Concept: Win in a Complex World*, TRADOC Pamphlet 525-3-1, Joint Base Langley-Eustis, VA: TRADOC, October 31, 2014, p. 18, hereafter TRADOC Pamphlet 525-3-1.

25. The symbiosis of humans and technologies is acknowledged as key in the Third Offset Strategy; see Katie Lange, "3rd Offset Strategy 101: What It Is, What the Tech Focuses Are," DoD

Live, posted March 30, 2016, available from *http://www.dodlive.mil/2016/03/30/3rd-offset-strategy-101-what-it-is-what-the-tech-focuses-are/*, accessed April 12, 2017.

26. Sandia National Laboratories website, available from *www.sandia.gov/radar/areas_of_expertise/analytics.html,* accessed on January 30, 2017.

27. Paul B. Symon and Arzan Tarapore, "Defense Intelligence Analysis in the Age of Big Data," *Joint Force Quarterly*, Vol. 79, October 1, 2015, available from *http://ndupress.ndu.edu/Media/News/Article/621113/defense-intelligence-analysis-in-the-age-of-big-data/,* accessed January 29, 2017.

28. Keir Giles and Kim Hartmann, "Shifting the Core: How emergent technology transforms information security challenges," *Datenschutz und Datensicherheit – DuD*, Vol. 41, Iss. 7, July 2017, pp. 434–439.

29. For example, a low-cost transmitting camera can be purchased at relatively low cost, see this example of an online retailer SpyCameraCCTV, available from *http://www.spycameracctv.com/spy/spy-cameras/home-office-spy-cameras/?gclid=CJOemr-3uNMCFRLgGwodJaEBEA*, accessed April 23, 2017.

30. Major Keith D. Anthony, U.S. Army Reserve, "Information Warfare: Good News and Bad News," *Military Intelligence Professional Bulletin*, January-March 1997, available from *http://www.fas.org/irp/agency/army/mipb/1997-1/anthony.htm*, accessed March 3, 2017.

31. Ranges of a kilometer can be achieved at low cost and in small form factor. See the following device example of a 3000m Remote Control Transmitter RF Radio Remote 315/433 Long Range Distance High Power Transmitter TX 1CH Big Button 2262, available to the public for purchase from AliExpress, available from *http://www.aliexpress.com/item/3000m-Remote-Control-Transmitter-RF-Radio-Remote-315-433-Long-Range-Distance-High-Power-Transmitter-TX/32246119234.html?spm=2114.40010308.4.2.FsLbsK*, accessed August 6, 2018.

32. Cori E. Dauber, *YouTube War: Fighting in a World of Cameras in Every Cell Phone and Photoshop on Every Computer*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2009.

33. Aden C. Magee, "Countering Nontraditional HUMINT Collection Threats," *International Journal of Intelligence and Counterintelligence*, 2010, Vol. 23, No. 3, pp. 509-520.

34. Justin R. Harber, "Unconventional Spies: The Counterintelligence Threat from Non-State Actors," *International Journal of Intelligence and Counterintelligence*, Vol. 22, No. 2, 2009, p. 231.

35. Giles, "The Next Phase of Russian Information Warfare," p. 9, referencing Ksenia Kirillova, "Rossiyskiye trolli terroriziruyut Zapad" ("Russian trolls terrorize the West"), Novyy (New) region 2, October 20, 2015, available from *from https://www.stopfake.org/rossijskie-trolli-terroriziruyut-zapad-ispolzuya-priemy-kgb/.*

36. Gordon Corera, "How France's TV5 was almost destroyed by 'Russian hackers'," BBC, October 10, 2016, available from *http://www.bbc.co.uk/news/technology-37590375*, accessed December 2, 2016.

37. Giles, "The Next Phase of Russian Information Warfare," pp. 3, 15.

38. Eugene Kiely and Lori Robertson, "How to Spot Fake News," Fact Check Org, November 18, 2016, available from *http://www.factcheck.org/2016/11/how-to-spot-fake-news/*, accessed February 19, 2017.

39. See the website of Integrity Initiative Defending Democracy against Disinformation, available from *http://www.integrityinitiative.net*, accessed April 22, 2017.

40. Jānis Bērzinš, "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy," Policy Paper No. 2, Riga, Latvia: Center for Security and Strategic Research, National Defence Academy of Latvia, 2014.

41. David E. Sanger and Scott Shane, "Russian Hackers Acted to Aid Trump in Election, U.S. Says," *The New York*

Times, December 9, 2016, available from *https://www.nytimes.com/2016/12/09/us/obama-russia-election-hack.html*, accessed June 5, 2017.

42. Harriet Agerholm, "Russian hackers penetrated Republican groups and campaigns, says FBI chief," *The Independent*, January 10, 2017, available from *http://www.independent.co.uk/news/world/americas/russian-hackers-fbi-penetrated-republican-cyber-attack-a7520261.html*, accessed June 6, 2017. See also Hunt Allcott and Matthew Gentzknow, "Social Media and Fake News in the 2016 Election," *Journal of Economic Perspectives*, Vol. 31, No 2, Spring 2017, pp. 211-236, available from *https://web.stanford.edu/~gentzkow/research/fakenews.pdf*, accessed June 6, 2017.

43. French Election: Emmanuel Macron condemns 'massive' hack attack," BBC, May 6, 2017, available from *http://www.bbc.co.uk/news/world-europe-39827244*, accessed June 6, 2017.

44. Bērzinš, p. 6.

45. "The Hybrid War Russia's Propaganda Campaign Against Germany," *Spiegel Online*, February 5, 2016, available from *www.spiegel.de/international/europe/putin-wages-hybrid-war-on-germany-and-west-a-1075483.html*, accessed May 11, 2017.

46. Ibid.

47. Ibid.

48. Patrick Sawer, "Russia accused of waging secret warfare against Britain using cyber attacks, espionage and fake news," *The Telegraph*, December 17, 2016, available from *http://www.telegraph.co.uk/news/2016/12/17/russia-accused-waging-secret-war-against-britain-using-cyber/*, accessed February 24, 2017.

49. Keir Giles, "Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power," London, UK: Chatham House, March 21, 2016, available from *https://www.chathamhouse.org/publication/russias-new-tools-confronting-west*, accessed May 25, 2017.

50. Peter Foster, "North Korea building secret ballistic missile submarine base," *The Telegraph*, July 22, 2016, available from

http://www.telegraph.co.uk/news/2016/07/22/north-korea-building-secret-ballistic-missile-submarine-base/, accessed March 2, 2017. See also Mark Hachman, "North Korean Gulags and 5 Other Secret Sites Exposed by Google Maps," *PC Magazine*, January 30, 2013, available from *http://uk.pcmag.com/gps-mapping-products/58154/gallery/north-korean-gulags-and-5-other-secret-sites-exposed-by-goog,* accessed on March 2, 2017.

51. Abdulkader Lamaa, Mark Jansen, Hugo Trépant, and Andrew Suddards, *Achieving information superiority Five imperatives for military transformation*, New York: Strategy& (formerly Booz & Company), Part of PwC network publication, 2014, available from *http://www.strategyand.pwc.com/media/file/Strategyand_Achieving-information-superiority.pdf*, accessed May 11, 2017.

52. Ian Tunnicliffe and Steve Tatham, *Social Media – The Vital Ground: Can We Hold It?* Carlisle, PA: Strategic Studies Institute, U.S. Army War College, April 2017.

53. Gosler, "Counterintelligence—Too Narrowly Practiced," p. 177.

54. J. Bowyer Bell, "Towards a Theory of Deception," *International Journal of Intelligence and Counterintelligence*, Vol. 16, No. 2, 2003, p. 278.

55. Giles, "Russia's 'New' Tools for Confronting the West," p. 31.

56. TRADOC Pamphlet 525-3-1, p. iii.

57. Bell, pp. 245-259.

58. Single and multiple outcomes are discussed at "*Artificially siloing* means *(projects) under* ends *(outcomes)* principle," DoView Visualizing Outcomes, n.d., available from *http://www.doview.com/outcomes-theory-simplified/p/siloing.html,* accessed on April 17, 2017.

59. Gosler, "Counterintelligence—Too Narrowly Practiced," pp. 173-174.

60. Ibid., pp. 173.

61. TRADOC Pamphlet 525-3-1, p. 18.

62. Gosler, "Counterintelligence—Too Narrowly Practiced," p. 182.

63. Keir Giles, "Assessing Russia's Reorganized and Rearmed Military," Washington, DC: Carnegie Endowment for International Peace, 2017, p. 6, available from *http://carnegieendowment.org/files/5.4.2017_Keir_Giles_RussiaMilitary.pdf*, accessed on May 29, 2017.

64. Giles, "Handbook of Russian Information Warfare."

65. Giles, "Russia's 'New' Tools for Confronting the West," p. 3.

66. Kim Hartmann and Keir Giles, "UAV Exploitation: A New Domain for Cyber Power," in N. Pissanidis, H. Rõigas, M. Veenendaal, eds., "2016 8th International Conference on Cyber Conflict: Cyber Power," Tallinn, Estonia: North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence Publications, 2016, available from *https://ccdcoe.org/sites/default/files/multimedia/pdf/CyCon_2016_book.pdf*, accessed June 6, 2017.

67. TRADOC Pamphlet 525-3-1, p. iii.

68. Ibid., p. i.

69. Joint Publication 3-13, pp. xii-xiv.

70. Ibid., pp. xi., I-5.

71. Field Manual 100-6, pp. 4-1, 6-4.

72. Joint Publication 3-13, pp. xii, xiv.

73. Field Manual 100-6, pp. 4-1, 6-4.

74. Joint Publication 3-13, p. II-10.

75. Ibid., p. IV-2.

76. Ibid., pp. x , II-1.

77. Jeffrey Goldstein, "Requisite Variety and the Difference that Makes a Difference: An Introduction to W. Ross Ashby's 'Variety, Constraint and Law of Requisite Variety,' Cybernetics, Regulation, and Complex Systems, Variety, Constraint, and the Law of Requisite Variety," in W. Ross Ashby, "Variety, Constraint and Law of Requisite Variety," *Emergence: Complexity & Organization*, Vol. 13, No. 1-2, 2011, pp. 190-200.

78. See Ken Thompson, "The law of requisite variety and team agility," The Bumble Bee: Ken Thompson's shared know-how on team dynamics, virtual collaboration, and bioteaming, October 22, 2007, available from *http://www.bioteams.com/2007/10/22/the_law_of.html*, accessed May 28, 2017.

79. A telling example is the socio-cyberattack on Estonia in May 2007. Primarily discussed in terms of a purely technical attack on information systems, during the event, the primary concern of the Estonian authorities was the concurrent Russian-inspired civil disorder.

80. This follows a discussion with staff at one of the UK's intelligence agencies.

81. The Technical Cooperation Program is an example of international collaboration, helping to reduce costs and share knowledge, see their website available from *http://www.acq.osd.mil/ttcp/*.

82. Brandon Pollachek, "New Army tool enhances electronic warfare capabilities," U.S. Army PEO IEW&S Public Affairs Office, March 2, 2015, available from *http://www.army.mil/article/143720/New_Army_tool_enhances_electronic_warfare_capabilities/*, accessed April 13, 2017.

83. Michael Dewar, *The Art of Deception in Warfare*, New York: Sterling, 1989, p. 195.

84. Gosler, "Counterintelligence—Too Narrowly Practiced," p. 182.

85. Giles, "The Next Phase of Russian Information Warfare," pp. 3, 12.

86. Joint Publication 3-13, p. 42.

87. For information about Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Policy (DOTMLPF-P) Analysis, see "JCIDS Process: DOTMLPF-P Analysis," AcqNotes, updated June 15, 2018, available from *http://www.acqnotes.com/acqnote/acquisitions/dotmlpf-analysis*, accessed August 3, 2018.

LIST OF ABBREVIATIONS AND ACRONYMS

ARCIC	Army Capabilities Integration Center
C2	command and control
C4ISTAR	command, control, communications, computers, information/intelligence, surveillance, targeting acquisition, and reconnaissance
DARPA	Defense Advanced Research Projects Agency
DoD	Department of Defense
EU	European Union
FBI	Federal Bureau of Investigation
HUMINT	human intelligence
IO	information operations
IPB	intelligence preparation of the battlefield
IRC	information related capabilities
ISIS	Islamic State in Iraq and Syria
ISTAR	intelligence, surveillance, target acquisition, and reconnaissance
IW	information warfare
MoD	Ministry of Defence
NATO	North Atlantic Treaty Organization
OPSEC	operational security
PLA	Chinese People's Liberation Army
SIO	special information operations
STO	special technical operations
UK	United Kingdom

U.S. ARMY WAR COLLEGE

Major General John S. Kem
Commandant

*****

STRATEGIC STUDIES INSTITUTE
AND
U.S. ARMY WAR COLLEGE PRESS

Director
Professor Douglas C. Lovelace, Jr.

Director of Research
Dr. Steven K. Metz

Authors
Dr. John A. S. Ardis
Dr. Shima D. Keene

Editor for Production
Dr. James G. Pierce

Publications Assistant
Ms. Denise J. Kersting

*****

Composition
Mrs. Jennifer E. Nevil

FOR THIS AND OTHER PUBLICATIONS, VISIT US AT

https://www.armywarcollege.edu/

ISBN 1-58487-790-1

This Publication

SSI Website

USAWC Website