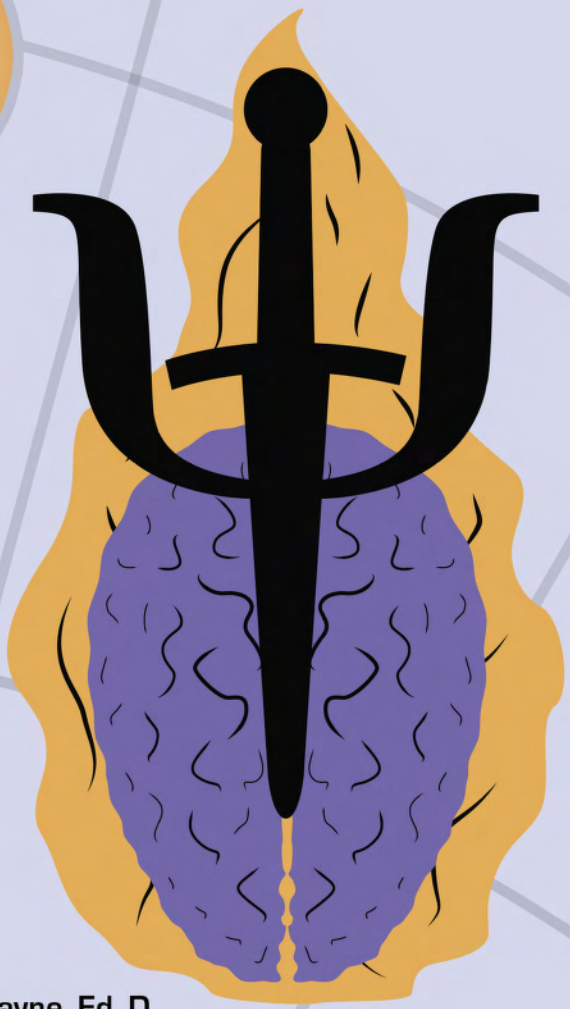
Volume 5, Number 1 Spring/Summer 2020

Global Security and Intelligence Studies Journal

The Emergence of the Psychological Warfighting Domain

Special Edition

Featuring an interview with Emerson Brooking, co-author of *LikeWar: The Weaponization of Social Media*



Editor-in-Chief — **Melissa Layne, Ed. D.**
Guest Editor — **Carter Matherly, Ph. D.**
Assisting Editor — **Joel Wickwire, MS**

ISSN: 2472-3614

Global Security and Intelligence Studies
Volume 5, Number 1 • Spring / Summer 2020

cont'd.

Book Reviews

Global Security and Intelligence Studies Journal

Volume 5, Number 1, Spring/Summer 2020

Special Edition

The Emergence of the Psychological Warfighting Domain

Global Security and Intelligence Studies is published by The Policy Studies Organization on behalf of American Public University System.

Aims and Scope. *GSIS* is a bi-annual, peer-reviewed, open access publication designed to provide a forum for the academic community and the community of practitioners to engage in dialogue about contemporary global security and intelligence issues. The journal welcomes contributions on a broad range of intelligence and security issues, and from across the methodological and theoretical spectrum. The journal especially encourages submissions that recognize the multidisciplinary nature of intelligence and security studies, and that draw on insights from a variety of fields to advance our understanding of important current intelligence and security issues. In keeping with the desire to help bridge the gap between academics and practitioners, the journal also invites articles about current intelligence and security related matters from a practitioner perspective. In particular, *GSIS* is interested in publishing informed perspectives on current intelligence and security related matters.

GSIS welcomes the submission of original empirical research, research notes, and book reviews. Papers and research notes that explicitly demonstrate how a multidisciplinary approach enhances theoretical and practical understanding of intelligence and security matters are especially welcome. Please visit https://www.ipsonet.org/publications/open-access/gsis/instructions-for-authors for complete details.

About the Cover. The cover design has four main elements- flame of knowledge and Promethus, brain, a weaponized Psi symbol, and global impact. From Greek Mythology Prometheus stole fire giving humans an advantage over the natural elements and a better understanding of the environment. A similar need for a basic understanding of the psychological Domain is necessary for in the current warfighting age. Centered within the flame of knowledge is a physical representation of the mental processes that control human behavior. This conveys the importance of understanding adversary behaviors, perceptions, and decision-making, as well as showing that human psychology is impacted by outside forces such as information, society, and culture. The weaponized Psi was an original design created by Dr. Carter Matherly to convey

strength and action in the Psychological Warfighting Domain with a nod to Psychological Operations (PSYOP) history for the US Armed Forces. The background depicts latitude and longitude lines to symbolizing the global impact and reach for the Psychological Warfighting Domain.

Cover Design by Caleb Osborn. A student at Clark State Community College in Springfield, OH and will complete his Associates of Applied Business in Graphic Design in the summer of 2020. He was introduced to the journal effort by his wife, who is an Information Operations Officer (14F) in the US Air Force, and has a background in Psychology. His current career goal after completing his degree is to work as Graphic Designer for an established company, eventually seeking a leadership role. He has over two years of experience working as a Graphic Designer, creating various designs for clients. He is passionate about providing creative design solutions.

Editorial Welcome

Greetings and welcome to the Spring/Summer 2020 issue of *Global Security and Intelligence Studies* Journal. This installation of GSIS is a special edition focusing on the emergence of the 6th warfighting domain; the Psychological Domain. This issue is very exciting and packed with insightful research, must read book reviews, policy recommendations, and an interview with Mr. Emerson Brooking, author of *LikeWar: The Weaponization of Social Media*.

The nature and execution of warfare has evolved throughout history. Warfare was once solely conducted through physical engagement of an enemy, armies dueling in will and might on the field of battle. Evolutions in technology introduced Naval and Air power to further influence and expand the battlefield. Most recently technology has opened the door to both Cyber and Space warfare. For the first time in history nations are able to leverage their might without the need for a physical presence or kinetic munitions.

Now, there is evidence supporting the weaponization of social connectivity and information sharing. The fundamental principles of psychology are being used as a weapon to inspire a nation's citizens against one another. In 2007 the world witnessed Estonia receive the first volley of attacks in an international cyber war. But another significant event occurred intertwined and largely unnoticed in the Bronze Revolution that shut down an entire nation. The battle was also the first instance of psychology employed as its own front on a multi-domain battlefield where no soldiers ever took up arms or held a line. Since this instance the employment of psychology as more than just a tool of conflict has grown in intensity and sophistication.

Scholars and practitioners alike have struggled to resolve the roles of psychology in modern warfare while being constrained with ideas, tools, and processes, intended for use in more traditional warfare. As a result fragmented terms such as the *Human Domain, Cognitive Domain, Information operations, Behavioral Domain,* and *Psychological Operations or Warfare* have made their way into both academia and some operational publications with little unifying and no clarifying efforts. It is the aim of this collection of research to draw a line in the sand and declare the formal establishment of the *Psychological Domain* as the 6th warfighting domain.

As the name implies Psychological encompasses each of the aforementioned bits of vernacular without unnecessarily limiting the scope or application of the domain. Terms such as *human*, *cognitive*, and *behavior* are all parts of the larger psychological field. Use of the term *psychology* may conjure images of the infamous Project MK-ULTRA or 'enhanced interrogations' used in the War on Terror. However, these examples highlight the need for specificity in terminology.

doi: 10.18278/gsis.5.1.1

Neither of these instances were informed by comprehensive, accurate, or substantiated psychological knowledge. Bringing unity to a severely fragmented capability will empower effectiveness in offensive and defensive operations across the spectrum of multi-domain operations.

The current COVID-19 pandemic highlights the critical need for unified efforts in the Psychological Domain. Claims of the virus being a bio-weapon, sanctions causing millions of deaths, and martial law all support themes of devising narratives not unlike those seen in recent political elections. Using Google Fact Checking Tool a 90 day review of 1,558 articles pertaining to COVID-19 presenting themselves as factual news was undertaken. The review revealed 1,240 completely false articles, 237 as misleading, and 25 as ambiguous. Only 36 of the original 1,558 were categorized as truthful. The remaining 16 articles were noted as being deliberately manipulative. The sheer numbers and blending of misleading, ambiguous, false, and manipulative data creates a brute force suppression of factual reporting.

This special edition opens with *The Case for the Sixth Domain of War: Psychological Warfare in the Age of Advanced Technology.* Authors Media Ajir and Bethany Vailliant make a captivating argument for the addition of a 6th domain of warfare. They draw focus to advancements in technology that makes access to populations easier, but psychological refinement of the message is still in need. As a result, efforts in the current 5 domain construct to influence a population are too compartmentalized to be effective.

Our second article, *Psychology as a Warfighting Domain* by a veteran intelligence team Sarah Soffer, Carter Matherly, & Robert Stelmack highlights the use of psychological operations throughout major historical conflicts. Through their research we are presented with an evolution of psychological warfare that notes its successes and failures. It closes with a synopsis of the modern information environment and signposts for the future in an interconnected world.

The third article in this special edition, *Discovering Influence Operations on Twitch.tv: A Preliminary Coding Framework* draws attention to how digital streaming platforms can and are being used as stages for influence operations. Authors Alexander Sferrella and Joseph Conger present a unique coding framework using Python scripting to help identify potential bots at rates faster and more accurately than human intervention.

Our fourth article takes aim at the propaganda efforts of one of the most active nations leveraging the Psychological Domain; Russia. Joseph Pagan highlights evolving political motivations of Russia's ruling elite in *A New Russian Realpolitik: Putin's Operationalization of Psychology and Propaganda*. The article discusses specific psychological theories that have been operationalized for use within the domain.

Our fifth article, *What's Thinking Got To Do With It? The Challenge Of Evaluating and Testing Critical Thinking In Potential Intelligence Analysts*, challenges intelligence practitioners and educators to consider the importance of critical thinking as a means to combat operations present in the Psychological Domain. Author Margaret S. Marangione reminds us that the best defense against weaponized information is applied cognition. Dr. Marangione makes her argument against the backdrop of critical thinking capabilities of younger generations and job placement testing.

Our final article in the special edition is brought to us by Jim Burch. His article *Reflecting History: The Basis for Assessing the Future* serves as a reminder that despite advances in technology and strategic thought, the basics still matter. While the intelligence community might currently prize analysts who have the ability to code and run scripts, the basics of historical and cultural understandings cannot be discarded. Dr. Burch notes how both historical and cultural understandings are intertwined with approaches to the psychology of an intelligence target, thereby broadening the basic skill set analysts need for success in an evolving environment.

We are also pleased to present a policy discussion from Jeremiah Deibler titled *Contesting the Psychological Domain During Great Power Competition*. His work highlights the need for a shift in strategic thinking to include the Psychological Domain in operational planning and execution. Resources and personnel must be dedicated to leveraging the benefits the Domain offers. His work makes the astute observation that message-centric operations are weapons with the potential to win conflict without the need for kinetics. However, the United States is in need of a unified force and planning cycle that can effectively fight in the domain.

Lastly, the special edition was humbled to have the opportunity to sit with Emmerson Brooking, Author of *LikeWar*, to discuss the evolution of warfare in the face of social media and the Psychological Domain. We close this edition with book reviews on three must have volumes for Intelligence practitioners. Austin Gouldsmith reviews *LikeWar: The Weaponization of Social Media, Messing with the Enemy* noting the dangers of social media and how it has been exploited for the benefit of global revisionist powers. Sara Soffer offers her review of *Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News* continuing the discussion on the perils of social media through the eyes of malicious actors. Joel Wickwire offers his keen insight in reviewing *The Conduct of Intelligence in Democracies: Processes, Practices, Cultures,* discussing the impact of intelligence operations on the global stage.

I sincerely hope you enjoy this special edition of *Global Security and Intelligence Studies* Journal. We set out to tackle a significant gap in both current academic literature as well as in the practice of warfare. Through the efforts of numerous talented individuals including authors, consultants, and subject matter experts we have been able to definitively establish and define a new warfighting domain

critical to academia, political, intelligence, military, and educational professionals alike. As a result we have presented a compelling argument detailing the critical need for the formal recognition of the Psychological Warfighting Domain. Thank you for being part of this journey.

In Arms,

Carter Matherly, Ph.D.
Guest Editor *Global Security and Intelligence Studies*

I would be remiss if I did not take a moment to thank the Editorial Staff of *Global Security and Intelligence Studies* including the many experts who contributed their time and efforts to see this edition and the included research come to reality. The Editor-in-Chief, Dr. Melissa Layne, thank you for the support and mentorship throughout the process of advertising, reviewing, compiling and publishing this special edition. Without your support or guidance this issue would not have come together so well, it has been an unprecedented honor and experience. A special thank you goes to Ms. Maryelizabeth Gano who was instrumental in introducing me to the staff of GSIS making this issue a possibility. Lastly a salute to all the members of the 14F community for your support and insight while developing this seminal volume.

Bienvenida editorial

Saludos y le damos la bienvenida a la edición Primavera / Verano 2020 de la revista *Global Security and Intelligence Studies Journal*. Esta instalación de GSIS es una edición especial que se centra en la aparición del sexto dominio de guerra; El Dominio Psicológico. Este tema es muy emocionante y está lleno de investigaciones perspicaces, debe leer reseñas de libros, recomendaciones de políticas y una entrevista con el Sr. Emerson Brooking, autor de *LikeWar: The Weaponization of Social Media.*

La naturaleza y ejecución de la guerra ha evolucionado a lo largo de la historia. La guerra una vez se llevó a cabo únicamente a través del compromiso físico de un enemigo, los ejércitos en duelo de voluntad y poder en el campo de batalla. La evolución de la tecnología introdujo el poder naval y aéreo para influir y expandir aún más el campo de batalla. Más recientemente, la tecnología ha abierto la puerta a la guerra cibernética y espacial. Por primera vez en la historia, las naciones pueden aprovechar su poder sin la necesidad de una presencia física o municiones cinéticas.

Ahora, hay evidencia que respalda el uso de armas de la conectividad social y el intercambio de información. Los principios fundamentales de la psicología se están utilizando como un arma para inspirar a los ciudadanos de una nación unos contra otros. En 2007, el mundo vio a Estonia recibir la primera descarga de ataques en una guerra cibernética internacional. Pero otro evento significativo ocurrió entrelazado y en gran medida desapercibido en la Revolución de Bronce que cerró una nación entera. La batalla también fue la primera instancia de psicología empleada como su propio frente en un campo de batalla multidominio donde ningún soldado tomó las armas o mantuvo una línea. Desde esta instancia, el empleo de la psicología como algo más que una simple herramienta de conflicto ha crecido en intensidad y sofisticación.

Los académicos y los profesionales por igual han luchado para resolver los roles de la psicología en la guerra moderna mientras se ven limitados por ideas, herramientas y procesos, destinados a ser utilizados en una guerra más tradicional. Como resultado, términos fragmentados como Dominio humano, Dominio cognitivo, Operaciones de información, Dominio conductual y Operaciones psicológicas o Guerra han llegado a la academia y a algunas publicaciones operativas con pocos esfuerzos unificadores y sin aclaraciones. El objetivo de esta colección de investigación es trazar una línea en la arena y declarar el establecimiento formal del Dominio Psicológico como el sexto dominio de guerra.

Como su nombre lo indica, Psicológico abarca cada uno de los fragmentos de lengua vernácula antes mencionados sin limitar innecesariamente el alcance o la aplicación del dominio. Términos como humano, cognitivo y de comporta-

miento son parte del campo psicológico más amplio. El uso del término psicología puede evocar imágenes del infame Proyecto MK-ULTRA o "interrogatorios mejorados" utilizados en la Guerra contra el Terror. Sin embargo, estos ejemplos resaltan la necesidad de especificidad en la terminología. Ninguno de estos casos fue informado por un conocimiento psicológico completo, preciso o comprobado. Llevar la unidad a una capacidad severamente fragmentada potenciará la efectividad en operaciones ofensivas y defensivas en todo el espectro de operaciones multidominio.

La actual pandemia de COVID-19 destaca la necesidad crítica de esfuerzos unificados en el Dominio Psicológico. Las afirmaciones de que el virus es un arma biológica, las sanciones que causan millones de muertes y la ley marcial respaldan todos los temas de la elaboración de narrativas no muy diferentes a las vistas en las recientes elecciones políticas. Con Google Fact Checking Tool se llevó a cabo una revisión de 9058 días de 1,558 artículos relacionados con COVID-19 que se presentaron como noticias objetivas. La revisión reveló 1.240 artículos completamente falsos, 237 como engañosos y 25 como ambiguos. Solo 36 de los 1,558 originales fueron categorizados como verdaderos. Los 16 artículos restantes fueron señalados como deliberadamente manipuladores. Los números absolutos y la combinación de datos engañosos, ambiguos, falsos y manipuladores crean una supresión de la fuerza bruta de los informes fácticos.

Esta edición especial comienza con *El caso del sexto dominio de la guerra: guerra psicológica en la era de la tecnología avanzada*. Los autores Media Ajir y Bethany Vailliant hacen un argumento cuidador para la descripción de un sexto dominio de guerra. Se centran en los avances tecnológicos que facilitan el acceso a las poblaciones, pero aún se necesita un refinamiento psicológico del mensaje. Como resultado, los esfuerzos en la construcción actual de 5 dominios para influir en una población están demasiado compartimentados para ser efectivos.

Nuestro segundo artículo, *Psicología como dominio de combate de guerra por un veterano equipo de inteligencia*, Sarah Soffer, Carter Matherly y Robert Stelmack destacan el uso de las operaciones psicológicas en los principales conflictos históricos. A través de su investigación, se nos presenta una evolución de la guerra psicológica que señala sus éxitos y fracasos. Se cierra con una sinopsis del entorno de información moderno y las señales para el futuro en un mundo interconectado.

El tercer artículo de esta edición especial, *La influencia de las operaciones en Twitvh.tv: un marco preliminar de coding* llama la atención sobre cómo las plataformas de transmisión digital pueden y están siendo utilizadas como etapas para operaciones de influencia. Los autores Alexander Sferrella y Joseph Conger presentan un marco de codificación único que utiliza secuencias de comandos de Python para ayudar a identificar posibles robots a velocidades más rápidas y más precisas que la intervención humana.

Nuestro cuarto artículo apunta a los esfuerzos de propaganda de una de las naciones más activas que aprovechan el Dominio Psicológico; Rusia. Joseph Pagan destaca las motivaciones políticas en evolución de la élite gobernante de Rusia en *Una nueva Realpolitik rusa: la operacionalización de la psicología y la propaganda de Putin.* El artículo analiza las teorías psicológicas específicas que se han puesto en funcionamiento para su uso dentro del dominio.

Nuestro quinto artículo, *¿Qué tiene que ver el pensamiento con eso? El desafío de evaluar y probar el pensamiento crítico en analistas de inteligencia potencial*, desafía a los profesionales y educadores de inteligencia a considerar la importancia del pensamiento crítico como un medio para combatir las operaciones presentes en el dominio psicológico. La autora Margaret S. Marangione nos recuerda que la mejor defensa contra la información armada es la cognición aplicada. La Dra. Marangione presenta su argumento en el contexto de las capacidades de pensamiento crítico de las generaciones más jóvenes y las pruebas de inserción laboral.

Nuestro artículo final en la edición especial nos lo trae Jim Burch. Su artículo Reflejando la historia: la base para evaluar el futuro sirve como un recordatorio de que, a pesar de los avances en tecnología y pensamiento estratégico, lo básico sigue siendo importante. Si bien la comunidad de inteligencia actualmente puede premiar a los analistas que tienen la capacidad de codificar y ejecutar guiones, no se pueden descartar los conceptos básicos de los entendimientos históricos y culturales. El Dr. Burch señala cómo los entendimientos históricos y culturales se entrelazan con los enfoques de la psicología de un objetivo de inteligencia, ampliando así las habilidades básicas que los analistas necesitan para tener éxito en un entorno en evolución.

También nos complace presentar una discusión sobre políticas de Jeremiah Deibler titulada *Cuestionando el dominio psicológico durante la competencia del gran poder.* Su trabajo destaca la necesidad de un cambio en el pensamiento estratégico para incluir el Dominio Psicológico en la planificación y ejecución operativa. Los recursos y el personal deben estar dedicados a aprovechar los beneficios que ofrece el Dominio. Su trabajo hace la astuta observación de que las operaciones centradas en mensajes son armas con el potencial de ganar conflictos sin la necesidad de cinética. Sin embargo, Estados Unidos necesita una fuerza unificada y un ciclo de planificación que pueda luchar eficazmente en el dominio.

Por último, la edición especial se sintió honrada de tener la oportunidad de sentarse con Emmerson Brooking, autor de LikeWar, para discutir la evolución de la guerra frente a las redes sociales y el dominio psicológico. Cerramos esta edición con reseñas de libros sobre tres volúmenes imprescindibles para los profesionales de inteligencia. Austin Gouldsmith revisa *LikeWar: The Weaponization of Social Media, Messing with the Enemy* notando los peligros de las redes sociales y cómo ha sido explotada en beneficio de los poderes revisionistas globales. Sara Soffer ofrece su reseña de *Surviving in a Social Media World of Hackers, Terro-*

rists, Russians, and Fake News, continuando la discusión sobre los peligros de las redes sociales a través de los ojos de actores maliciosos. Joel Wickwire ofrece su perspicacia al revisar La conducta de la inteligencia en las democracias: procesos, prácticas y cultura que discuten el impacto de las operaciones de inteligencia en el escenario global.

Espero sinceramente que disfrute de esta edición especial de la revista *Global Security and Intelligence Studies Journal.* Nos propusimos abordar una brecha significativa tanto en la literatura académica actual como en la práctica de la guerra. A través de los esfuerzos de numerosas personas con talento, incluidos autores, consultores y expertos en la materia, hemos podido establecer y definir definitivamente un nuevo dominio de combate crítico para profesionales académicos, políticos, de inteligencia, militares y educativos por igual. Como resultado, hemos presentado un argumento convincente que detalla la necesidad crítica del reconocimiento formal del dominio de lucha psicológica de guerra. Gracias por ser parte de este viaje.

En armas,

Carter Matherly, Ph.D.

Editor invitado *Global Security and Intelligence Studies*

Sería negligente si no me tomara un momento para agradecer al Equipo Editorial *Global Security and Intelligence Studies*, incluidos los muchos expertos que contribuyeron con su tiempo y esfuerzos para ver esta edición y la investigación incluida hacerse realidad. La Editora en Jefe, Dra. Melissa Layne, le agradece el apoyo y la tutoría durante todo el proceso de publicidad, revisión, compilación y publicación de esta edición especial. Sin su apoyo u orientación, este problema no se habría unido tan bien, ha sido un honor y una experiencia sin precedentes. Un agradecimiento especial a la Sra. Maryelizabeth Gano, quien fue instrumental en presentarme al personal de GSIS haciendo posible esta cuestión. Por último, un saludo a todos los miembros de la comunidad 14F por su apoyo y conocimiento mientras desarrolla este volumen seminal.

The Case for the Sixth Domain of War: Psychological Warfare in the Age of Advanced Technology

Bethany Vailliant and Media Ajir

Abstract

Wills win wars. A country at war must have and maintain the support of its people to achieve victory. Targeting will, using advanced information technology (IT), presents a new vulnerability for the United States. Literature in this field has largely ignored the psychological effects of new, cyber-enabled tools; therefore, the concept of information warfare has tended to favor primarily technical infrastructure. This oversight has caused state mismanagement of what was once carefully managed disruption by the United States. Tools and techniques have been refined to transcend effects beyond material goods, entering our minds and manipulating our behavior. The weaponization of these tools urges us to consider the sufficiency of our current framework for warfare—the five domains. This research argues that due to the disruptive change in the delivery method of information, a sixth, psychological domain should be established to properly assess and operationalize effects going forward.

Keywords: cyberspace, psychological domain, psychological warfare, information warfare, fifth domain, sixth domain

El caso del sexto dominio de la guerra: guerra psicológica en la era de la tecnología avanzada

Resumen

Las voluntades ganan guerras. Un país en guerra debe tener y mantener el apoyo de su gente para lograr la victoria. La focalización, utilizando tecnología de información avanzada, presenta una nueva vulnerabilidad para los Estados Unidos. La literatura en este campo ha ignorado en gran medida los efectos psicológicos de las nuevas herramientas cibernéticas; por lo tanto, el concepto de guerra de información ha tendido a favorecer principalmente la infraestructura

 doi: 10.18278/gsis.5.1.2

técnica. Este descuido ha provocado una mala gestión estatal de lo que antes era una interrupción cuidadosamente manejada por Estados Unidos. Las herramientas y técnicas se han refinado para trascender los efectos más allá de los bienes materiales, entrar en nuestras mentes y manipular nuestro comportamiento. El armamento de estas herramientas nos insta a considerar la suficiencia de nuestro marco actual para la guerra: los cinco dominios. Esta investigación argumenta que, debido al cambio disruptivo en el método de entrega de información, se debe establecer un sexto dominio psicológico para evaluar y operacionalizar adecuadamente los efectos en el futuro.

Palabras clave: Ciberespacio, dominio psicológico, guerra psicológica, guerra de información, quinto dominio, sexto dominio

第六战争领域案例：先进科技时代下的心理战

摘要

意志赢得战争。战争中的国家必须拥有人民支持，并保持这种支持以获得胜利。使用先进信息技术对意志发起攻击，为美国增添了一个新的弱点。该领域文献在很大程度上忽视了新型网络工具带来的心理效果；因此，信息战概念往往主要偏好技术基础设施。这一疏忽已导致各州在信息中断方面管理不善，后者曾一度由美国仔细管控。工具和技术经过改良，产生的影响已超越有形物品，进入我们的思维并操纵我们的行为。这些工具的武器化敦促我们衡量当前对五个战争领域所提出的框架的充足性。本研究主张，鉴于信息交付方式中的破坏性变化，应建立第六领域，即心理领域，以对未来产生的效果进行正确评估和操作化。

关键词：网络空间，心理领域，心理战，信息战，第五领域，第六领域

Introduction

As warfare has modernized, its disruptive nature continues to take advantage of advanced technologies, especially those within the information sphere. According to the Department of Defense (DoD), "Information is a powerful tool to influence, disrupt, corrupt, or usurp an adversary's ability to make and share decisions" (Joint Chiefs of Staff 2014).

Such disruptions began with the invention of mass printing in the fifteenth century, when books became available to large swaths of people, arguably igniting civilization's leap forward into the current era, "including but not limited to the Reformation, the Enlightenment, the steam engine, journalism, modern literature, modern medicine, and modern democracy" (Marantz 2019).

While the chains that shackled the free flow of information were coming undone, so too did misinformation break free as its opposite. The gatekeepers of knowledge started to shift from princes and priests, to new entrepreneurs who had the financial means to access and purchase the powerful new technology of the printing press.

In the twentieth century, with the advent of the internet, new liberators of information have emerged. The dawn of this new era was described with the same excitement as that of the printing press. Unlike the print media however, where gatekeepers—and the law in many places—had final say on what was published and what was not, this new means of information sharing was unregulated/under-regulated and full of advocates for an internet based on the liberation of knowledge and power. However, while stakeholders in this era have debated the antiquities of free speech and its nuances, what has been ignored almost entirely is the potential for a new kind of warfare targeting the human mind, amplified by new technology and tools of communication.

Over the years, while the United States has been building up its unmatched and largely physical military strength, its adversaries have been busy searching out and filling whatever asymmetric power gaps they are able. As we argued in our previous article, *Russian Information Warfare: Implications for Deterrence Theory*, a common development of state actors with fewer defense resources has led to the development of tools of power that are low cost and high impact (Ajir and Vailliant 2018). The United States (and many other Western states for that matter) is still unprepared to deal with this new reality.

The Joint Chiefs of Staff (2014) clearly call out the problem:

> The instruments of national power (diplomatic, informational, military, and economic) provide leaders in the United States with the means and ways of dealing with crises around the world. Employing these means in the information environment requires the ability to securely transmit, receive, store, and process information in near real time. The nation's state and non-state adversaries are equally aware of the significance of this new technology, and will use information-related capabilities (IRCs) to gain advantages in the information environment, just as they would use more traditional military technologies to gain advantages in other operational environments. These realities have transformed the information environment into a battlefield,

which poses both a threat to the Department of Defense (DOD), combatant commands (CCMDs), and Service components and serves as a force multiplier when leveraged effectively.

This paper argues for the recognition of a new, psychological domain in order to create the framework to understand the target effects of such new tools. The **delivery method** for information is rapidly changing, making its potential **effects** more detrimental and/or lethal, especially in a world of reemerging great power competition. Therefore, the establishment of a sixth domain of warfare is necessary as we move forward into the twenty-first century. In order to make the case for its recognition, we will define the necessary components of a domain, identify where the cyber domain ends and where the psychological domain begins, and illustrate the implications of advanced technology on warfare in the new domain. At its core, this research seeks to explore why a psychological domain has not yet been recognized, and to argue that the time to do so is now.

Information Operations in the Age of Advanced Technology

The United States' military superiority has largely been defined by its unique ability to navigate and dominate its enemies in the classical domains of warfare. Military operations have fundamentally changed throughout the twentieth century to adapt to new technologies. Historically, operations were dominated by the two domains of land and sea. The advent of powered flight in 1904 resulted in the creation of the third domain, air, and fifty years after the first powered flight, the US Air Force was born. The space domain was acknowledged not long after, with the advent of Ronald Reagan's Strategic Defense Initiative in the 1980s (Allen and Gilbert 2018). Finally, the Pentagon's declaration of cyberspace as the fifth domain of warfare came after a massive DoD network compromise in 2008 (Horning 2011).

Despite the importance of domains to war, a clear and concise definition does not seem to have been put forth in military doctrine. We recognize that the very concept of "domain" may be problematic to some, as they all cannot be compared equally. The conventional domains of air, land, and sea are certainly more physical in nature than the cyber domain and, while space may also be physical, it has so far proven to be most useful for virtual enabling effects, such as communication, surveillance, and navigation (Heftye 2017). However, "domain" has become such an embedded concept in military thinking that we do not wish to debate its value as a construct. Therefore, we put forward the definition by Patrick Allen and Dennis Gilbert of Johns Hopkins University for consideration:

1) It is a sphere of interest

2) It is a sphere of influence in that activities, functions, and operations can be undertaken in that sphere to accomplish missions

3) It is a sphere that may include the presence of an opponent

4) It is a sphere in which control can be exercised over that opponent.

All of the war domains are nested within the larger information environment. The use of information during wartime or in peacetime operations is not unique to any of the domains. The objective when conducting information operations in any of the domains is to deny, corrupt, or destroy an adversary's information and systems, to defend our own, and to exploit available information to enhance the decision cycle and achieve information superiority (Kovacich and Jones 2006). The Joint Chiefs of Staff (2019) define "information environment" as:

> The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.

Furthermore, it defines "information operations" as:

> The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.

More broadly, "information warfare" generally comprises three functional areas:

- electronic warfare (e.g., jamming communications links, eavesdropping of signals)
- network warfare (where computer networks are the weapons and targets)
- psychological operations (which aims at altering the perceptions of the target audience to be favorable to one's objective) (Brazzoli 2007)

Where the Cyber Domain Begins and Ends

Mapping out cyberspace can assist in visualizing the fifth domain (see Appendix 1). Cyberspace is generally viewed as three layers: physical, logical, and social. Within these three layers are five components: geographic, the physical network, the logical network, cyber persona, and persona. The geographic component refers to the physical location of network elements. The physical network components include all of the hardware and infrastructure required for network operability. The logical layer is technical in nature and consists of the logical connections that exist between devices. The social layer consists of cyber personas, referring to identification on a network, such as email addresses or computer IP addresses, and personas, meaning the actual person behind the network. This top social layer is obviously required, as the fifth domain cannot be navigated without end-to-end users. However, operations conducted with targets in the cyber domain allow only for the effects of the two functional areas of electronic and network warfare, excluding the effects of psychological operations.

The Joint Chiefs of Staff (2019) define "cyberspace" as:

> A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

The tendency to artificially view acts that occur in cyberspace as automatically constituting network and electronic warfare excludes the impacts of virtual connectivity that extend far beyond the underlying infrastructure that makes its existence possible. This, we believe is the first mistake—nowhere in the definition of cyberspace are the human-related tools and effects included. In order to begin untangling the cyber domain from the others, it is first important to understand exactly what the larger objectives of cyber warfare by itself are, and consequently what they are not.

RAND defines "cyber warfare" as follows:

> The actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.

Cyberwar and its effects, as defined by the DoD, occur exclusively within the cyber domain, and are by their very nature inseparable from the information systems that magnify the impacts of war in the information environment. Attacks on critical infrastructure (such as railways, hospitals, stock exchanges, airlines, financial systems, oil pipelines, water distribution systems, electric grids, etc.), distributed denial of service (DDoS) attacks (online banking, digital news media, government websites, etc.), malware, ransomware, and data deletion are some of the most prominent examples of methods used to conduct an attack in the cyber domain (Greenberg 2019). The objective of an attack in the cyber domain is to directly target the information itself or the systems on which the information resides.

According to the Geneva Centre for Security Sector Governance, Computer Network Operations (CNO) are comprised of three forms: 1) computer network attacks, which are operations designed to disrupt, deny, degrade, or destroy information on computers or computer networks or the computers or networks themselves, 2) computer network exploitation, which is the retrieving of intelligence-grade data and information from enemy computers by ICT means, and 3) computer network defense, which consists of all measures necessary to protect one's own ICT means and infrastructures. All three CNO forms of activity can take place within cyberspace in a manner that does not rise to the level of impact necessary to constitute an attack or warfare.

While the impacts from cyber warfare are potentially many, the underlying threat that ultimately emanates

from war in the cyber domain is our ever-increasing dependence on the electromagnetic spectrum (EMS), which is the foundation upon which entrance into the virtual space and the storage of information is possible (Schreier 2015). It is the targeting and exploitation of this underlying technological infrastructure that makes the cyber domain distinct from the other domains. The modern world has become so reliant upon cyberspace for all aspects of life that the loss of the ability to operate in cyberspace is potentially crippling in all domains. Indeed, cyberspace enables faster and more efficient transmission of information within and across all of the other domains. Networks, information technology (IT) systems, and computer databases enable national leadership and the military to create a higher level of shared situational awareness, to better synchronize command, control, and intelligence, and to translate information superiority into combat power (Schreier 2015). All types of national-level operations are increasingly reliant on the use of data and information, and virtual transmission through cyberspace allows its ingestion and analysis, sometimes almost instantaneously.

Therefore, we believe that the definition of "cyberspace" offered by the DoD needs to be expanded. While it does correctly state that cyberspace is a part of the broader information environment, its second mistake is that it does not recognize its role as a force multiplier that enhances the effectiveness of the information environment as a whole. For this reason, we offer the following to accurately reflect the true nature of the role of cyberspace:

> A global domain that operates within, **and as an enabler of**, the information environment through the use of the information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.

As a result of cyberspace's role in enhancing the effectiveness of the information environment, subsequent cyber-enabled delivery methods of information will continue to evolve. This means effects for psychological operations will require their own domain and the definition of cyberspace will not need to include human-related tools and effects. This is precisely where the cyber domain ends, and where the psychological domain begins. Because while the distinguishing feature of war in the cyber domain is its targeting of the structures that enable cyberspace to function, war in the cyber domain does not include the influence operations that seek to, for example, spread disinformation and propaganda or hurt adversaries by leaking damaging information about them (Greenberg 2019).

Where the Psychological Domain Begins

The human dimensions of information have always existed within the information environment. Often called by another name, "psychological operations" (or PSYOPS) have

often been recognized as one of the core components of information warfare. If psychological operations occur within the human mind and have always existed, why has it not been officially recognized as a domain of war? The answer is that historically, as an instrument of war, influencing public opinion within an enemy state was expensive, slow, data-poor, and attributable (Hwang and Rosen 2017). This is no longer true, and the reason admittedly has everything to do with cyberspace and its underlying foundation of advanced technology.

The combined use of technology with these human-related dimensions exponentially amplifies the influence that a message has on decision-making. If cyber-enabled psychological operations are undertaken with the objective of achieving information superiority, the effects will not be found within cyberspace—they will be found in the sixth, and currently unrecognized psychological domain. While the ultimate target in the cyber domain is the underlying EMS that makes up our virtual world and everything that depends on it to work, it is within the psychological domain that the human mind is targeted through constantly evolving methods of cyber-enabled psychological warfare.

It is important to note that the sixth domain should be called the psychological domain, rather than the cognitive domain. Cognition is "the mental action or process of acquiring knowledge and understanding through thought, experience, and the senses" (*Oxford Online Dictionary*, s.v. "cognition," https://www.lexico.com/en/definition/cognition). This involves the biological and neurological processes linked to attention, executive function, memory, visuospatial function, and language. In contrast, psychological refers to "of, affecting, or arising in the mind; related to the mental and emotional state of a person" (*Oxford Online Dictionary,* s.v. "psychological," https://www.lexico.com/en/definition/psychological). Cognition can be viewed as a faculty of being human that is one aspect of psychology studies. This distinction is important because cyber-enabled information warfare does not attack *only* the underlying cognition of the human brain, but the broader psychology of an individual, including their mental state; perception; cognitive, emotional, and social processes; and behavior. Furthermore, there is a body of research that illustrates how the growing use of technology can affect human cognitive abilities (Wilmer, Sherman, and Chein 2017), such as attention span and memory. Therefore, our cognition is being targeted as an indirect result of peoples' increasing reliance on technology, making us more vulnerable to future targeted cyber-enabled psychological operations.

Using Allen and Gilbert's proposed definition and subsequent components of a domain, the psychological domain has all the required characteristics to be formally recognized. First, the human mind is a sphere of interest for those inclined to manipulate its decision-making processes, behaviors, and emotions. Second, within this sphere, activities, functions, and operations

can be undertaken to accomplish missions—these actions have existed since the beginning of humanity and have exponentially increased along with the expansion of technology. Third, it is a sphere that may include the presence of an opponent—adversaries are increasingly using information operations to gain an advantage within the human mind. Lastly, it is a sphere in which control can be exercised over an opponent, as information warfare tactics aim to deceive, manipulate, and control an opponent's decisions or lack thereof.

In the second component, the psychological and cyber domains are intertwined, making their distinction difficult. This is because the activities, functions, and operations undertaken to influence the human mind in the psychological domain are occurring through cyberspace in the modern information environment (refer to the social layer of cyberspace in Appendix 1). This may be difficult to understand in the traditional sense, since the classical domains of warfare tend to lend themselves to easy delineation. For example, tanks conduct ground warfare, ships belong in the ocean, and planes fly in the air; however, even these relatively straightforward examples demand some scrutiny. All domains have entry and exit points into other domains at some point. Aircraft land on the ground or at sea, and ships dock at land-based ports. Warheads enter space before making their reentry to hit their land-based targets. This differentiation becomes more important as we move away from traditional warfare and towards the more convoluted, virtual spheres of influence. The sphere of influence where the effects actually take place and the end objective are always more important when assigning an operation to a domain of war than whatever activities are necessary to achieve it.

Information can be defined in two ways: facts provided or learned about something or someone and what is conveyed or represented by a particular arrangement or sequence of things (in computing, this is data as processed, stored, or transmitted by a computer). In fact, in Late Middle English, information was known as the "formation of the mind" (*Oxford Online Dictionary*, s.v. "information," https://www.lexico.com/en/definition/information). As stated previously, the information environment is a sphere in which all domains operate. Figure 1 illustrates our proposed model of how information, whether delivered through virtual or non-virtual methods, can be transported and have psychological effects. This manner of visualizing our theory is two-fold. First, it allows cyber-enabled psychological operations to be carried out within its own domain and its effects to have a home. Second, it demonstrates that without a human to cognitively observe and infer what is happening (a cognitive maneuver), none of the other domains matter, and arguably, without people writ large applying their cognition, those domains arguably do not exist. This illustrates that targeting the psychological domain can impact all actions in the other domains downstream.

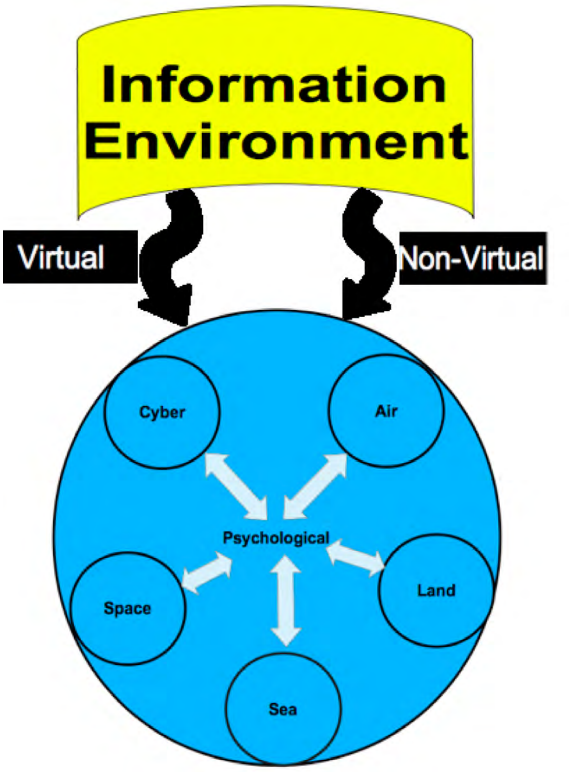


Figure 1. The information environment spans across all war domains, enhanced by the use of cyber-enabled (virtual) delivery methods.

Cyberspace gives states and independent groups a **direct pathway into the hearts and minds of individual citizens through the internet.** For this reason, "cyber-enabled" psychological war in the psychological domain shares many characteristics of the cyber domain, such as low cost of entry, the ability to be endlessly replicated, the difficulty of attribution, and the odds currently being in favor of the offense over the defense. Within the larger information environment, activities undertaken in cyberspace are a pathway into the human mind, enhancing, but not solely enabling, the activities, functions, and operations that an adversary undertakes to achieve its objectives. Just as an intercontinental ballistic missile allows nuclear warheads to be guided to their targets thousands of miles away, the internet allows messages to be carried across oceans right into our pockets. This analogy, although oversimplified, is no less powerful—methods of delivery that minimize the time it takes and the distance a message has to travel can create catastrophic outcomes for those on the receiving end. Regardless of the way that information travels, however, the most important consideration should always be what end-state the adversary intends to create to achieve its overall mission.

Methods of Cyber-Enabled Psychological Warfare

In his book *Thinking, Fast and Slow*, Daniel Kahneman argues that the way the human mind deals with information is broken down into two systems: "System 1" and "System 2." System 1 operates automatically and quickly, with little or no effort and no sense of voluntary control; System 2 allocates attention to the mental activities that demand it, including complex computations. System 1, while useful to people as a way to deal with the chaos of the world around them, is often overrun with subconscious biases. Ideally, that is when System 2 steps in to correct the mistakes of System 1; however, according to Kahneman (2011), "constantly questioning our own thinking would be impossibly tedious, and System 2 is much too slow and inefficient to serve as a substitute for System 1 in making routine decisions."

Applying Kahneman's two systems theory to the psychological domain illustrates how cyber-enabled information warfare tactics can take advantage of the inherent weaknesses of the human mind to further agendas and influence the perceptions and actions of individuals in the real world. There are four main types of cyber-enabled methods that can influence the human mind in a way that makes it rely on the quick and impulsive tendencies of System 1 rather than System 2.

1) Disinformation dissemination via the internet

As previously noted, the concept of disinformation is not a new phenomenon. It is also important to note that "online disinformation specifically and narrowly refers to information that is demonstrably false and deliberately spread on the internet with the intention of shaping public opinion. This separates it from 'misinformation' which is false information, but that may not be deliberately so" (Raderstorf and Camilleri 2019). Previous tactics of dissemination of false information included newspapers, broadcasting, leaflets, etc. Twenty-first century information warfare now includes the internet, in particular social media—cyberspace's premier host for social interaction. With its existence comes a number of distinct characteristics that can be categorized as both benefits and vulnerabilities, depending on which side you are on.

- The **speed**_by which the rate of disinformation delivery has exponentially increased via cyberspace, especially through social media. Algorithms have been designed to increase views and shares, quickly making stories go viral (Nemr and Gangware 2019), and automated bot armies can deliver volume and repetition at high speeds to amplify messages (Adams 2018).

- The **ease of this delivery method** has exponentially increased. One post can reach millions of targets because as an online post is not scalable; it takes the same amount

of effort to reach one person as it does five million (Shallcross 2017). Conversely, the simplicity by which information is shared has led to **increased accessibility** by those on the receiving end.

- **Attribution** in this arena is increasingly difficult. Social personas can create profiles that appear to be legitimate, but in reality are fake. Websites can also be created by unknown sources to relay disinformation. Furthermore, the narratives do not necessarily have to be untrue. For example, they can be attached to already-established movements within a democratic society. The impact of this is twofold: first, it gives artificial credibility and visibility to otherwise illegitimate groups. Second, if the deception is detected, it can have the opposite effect of discrediting legitimate groups by tainting them with foreign interference.

- There is an **ever-growing information environment**. Information overload can lead to mass confusion and the subsequent disengagement of society, making information manipulation by the aggressor easier and more normalized. The "velocity of human interaction and the velocity of information is at an all-time high," leading to somewhat of a truth crisis (Banach 2018). Even if there is an overall awareness of deception by the public and the individuals that comprise it, the limitations of System 2 to handle so much information means that corrections and fact checking almost never fully undo the damage done (Kagan, Bugayova, and Cafarella 2019).

2) Cyber Espionage

While there is no agreed upon definition at the moment, the 2013 Tallinn manual defines cyber espionage as "an act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party" (Schmitt). These hacking operations are typically carried out by nation states, but are increasingly taken up by non-state actors. Conversely, "hacktivism" blends hacking and activism for a political or social cause, and state and local governments are increasingly finding themselves targets (Bergal 2017). This form of digital disobedience, however altruistic the intent, is highly disruptive and regarded as harassment.

While there are a variety of ways hacked information can be used to influence targets, one tactic is hack and leak operations. This involves two stages: the first "focuses on intrusion (unauthorized access to networks), while the second concentrates on influence (the use of digital technologies to shift public debate) (Shires 2019). The intrusion into specific digital systems and networks constitutes cyber espionage—the theft of information in cyberspace, usually classified as compromising material. On the other hand, the leak of said stolen information into the public arena has intended psychological effects. This is perhaps especially so when the

release of documents is promulgated in a meticulous fashion, to achieve heightened effects and reactions. James Shires (2019) argues that hack and leak operations are *mechanisms of delegitimization*, based on their technical characteristics, social and political context, and target audiences. This conceptualized framework advances our argument for a sixth domain: the effects of a cyber-operation such as cyber espionage can reach far beyond the intrusion itself and into the realm of public consciousness.

3) Technical Disruptions

Technical disruptions typically involve the hindrance and/or suspense of activities in cyberspace in order to degrade operational effectiveness, which inevitably leads to emotional frustration. This activity includes causing glitches in IT to influence emotions, motives, and objective reasoning. Ultimately, the behavior of an operative becomes less efficient and effective in performing their own cyber missions in a manner favorable to their objectives. Much of this effort focuses on "creating an endless series of technology annoyances and time-wasting interruptions that degrade and disrupt the workflow of network operators significantly" (Lin 2020). These methods involve the usage of cyberspace to affect the brain and, by extension, behavior.

4) Precision Target identification through use of data and predictive analytics

This tactic refers to acquiring data that exhibits user habits online to precisely target victims more likely to be impacted by actions to drive and manipulate behavior. It allows for building insight from analysis of data collected through online interactions and engagements to form predictions about future behavior. Artificial intelligence trained with data from users' social media accounts, economic media interactions (Uber, Apple Pay, etc.), and their devices' geolocation can infer predictive knowledge of its targets (Telley 2018). A commercial example to illustrate this technique is the new phenomenon of using consumer data habits to drive real time automated bidding on personalized advertising—otherwise known as "programmatic advertising." It is only a matter of time before nation states begin to weaponize this technique, particularly in elections and civic engagement (Patterson 2019).

Why Recognition of the Psychological Domain Matters

The distinguishing feature of war in the psychological domain is the targeting of human decision-making. Information often empowers people and enriches their lives, and the internet enhances it by providing ever-greater access to new knowledge, business, and services; however, there is a downside to virtual space as well. Many topics in the social sciences are approached with the assumption that people are "rational actors," but our adversaries approach war in the cognitive domain knowing full well that the opposite is often much closer to the truth. People are not simply rational processors of information, and

cyber-enabled psychological warfare takes advantage of the vulnerabilities created by the limitations of the human mind. These same individuals are what constitute the core of democratic societies, making this issue fundamental to the United States. However, defending democracy is not just a job that falls to individuals or to businesses—it is a national security issue that demands the attention and resources of our defense infrastructure.

First, the establishment of the psychological domain will undoubtedly encourage investment in further research, discussion, and resources, including personnel and appropriate infrastructure. In conflict, there is always an advantage to the side that understands and operates within a domain better than the opponent (Allen and Gilbert 2018). Distinguishing effects carried out within domains in the information environment allows for the proper framework to carry out and assess operations, while sharing best practices. Planners and decision-makers can strengthen the effectiveness and efficiency of these operations, using common language, methods, and capabilities. The US government needs to devote substantially more effort to understanding the science and practice of psychological operations, as they are not synonymous with cyber operations. Cyber operations are intended to hack silicon-based processors and technology, while psychological operations are intended to hack carbon-based processors—that is, human brains. If an organization's expertise is primarily with the former, how can it execute operations intended to optimize the outcomes of the latter (Lin 2020)? What is required is expertise on social cognition and behavioral economics—the fundamental psychological science underlying influence campaigns—along with social network analysis, decision analysis, and the human aspects of command and control.

By recognizing the psychological domain, it gives credibility to the idea and will lead to the further development of a body of literature on the subject and, ultimately, a deeper understanding of the problem. This is not just exclusive to the United States, but could be an international effort as well. When the United States recognized cyber as a domain, NATO soon followed suit, and a vast amount of research naturally followed thereafter. This does not necessarily mean there will be an immediate consensus, but in the case of the cyber domain, it created a legitimate space to begin the development of a broader conversation. In many ways, this conversation has already begun; however, as we have argued throughout this paper, the conversation is not being framed effectively. The way that the government frames national security issues often has a substantial impact on how organizations that are trying to offer their support or on how academics trying to add to the literature put forth their own contributions. The fact that the United States, and many other Western states, draw upon the public's knowledge as input to the larger policy discussion is a strength that many of our adversaries do not take advantage of. There is incredible potential in en-

gaging with the broader community to find ways of combating this new and unique threat.

Second, the establishment of the psychological domain is critical because democratic governance relies on reliable and trustworthy information for people to make rational and calculated decisions. Yet, cyber-enabled war in the psychological domain allows for the spread of falsehoods and the sowing of chaos that distorts reality and degrades trust. As it stands, foreign influence and interference pose a significant threat to democracy. Whether it be through pure cyber-attacks on a state's infrastructure or disinformation campaigns, adversaries are seeking to divide our societies and degrade confidence not only in elections, but also in the overall credibility of our institutions. Adversaries will continue to adopt and look for ways to weaken the United States and its allies, strengthening their own strategic position on the world stage. This will be an ongoing intrusion that knows no borders, infringing on the functioning of democracies worldwide.

Third, the establishment of the psychological domain will send a signal to our adversaries, initiating digital deterrence. As we argued in our previous article, the weaponization of information changes the application of deterrence, both within the cyber domain and the psychological domain (Ajir and Vailliant 2018). Elements of deterrence will be applied to each domain differently, hence changing its applicability. In an era of great power competition, US strategic deterrence will need to evolve to encompass warfare in all domains, including the psychological domain. However, we must take a few steps back and understand that we cannot meaningfully deter our adversaries unless they are aware of our capabilities; these capabilities will not be fully developed unless the sixth domain is established.

Conclusion

In her 1979 book *The Printing Press as an Agent of Change,* Elizabeth Eisenstein acknowledges the profit motive that drove many early printers and the fact that disinformation and propaganda was still rife. However, she argues that despite the downsides, such as heightened ethnic tensions, the spread of medical disinformation, and about a century's worth of European religious wars, the long game was more important. In other words, "even when early printing technology ought to be described as a weapon, Eisenstein treats it more like a light bulb" (Marantz 2019). But what happens when modern technology completely changes information dissemination? Will the light bulb continue to illuminate, or will it be dropped and burn everything to the ground? Or perhaps, if not guided, it will shine a glaring light on the ugliness beneath the social cohesion of contemporary society. This is why establishing a sixth domain is necessary—it will lead to a more comprehensive understanding of the effects of cyber-enabled psychological attacks on the human psyche, subsequently leading to policies in de-

fense of our nation. It means taking the downside risks of the light bulb more seriously, and with a bit more caution, as the long game is more important.

It may seem paradoxical, as some may argue that acting in this sixth domain will make us no better than Russia or China—two anti-democratic regimes, competing to be great powers. We counter that the United States exemplifies the democratization of information—upholding liberal values of democracy including free speech and the free flow of information, something Russia and China and many other authoritarian regimes do not allow. Both states use information operations domestically to suppress dissent and control what people think, whether through manipulation or censorship, all while exporting a particular model of digital authoritarianism globally. Russia and China illustrate the unintended consequences of the digital information age—the new paradigm scholars once thought would give more power to the people is instead being used to silence and control them. Our adversaries have weaponized information to control behavior both at home and abroad, as a method of normal politics, while Western democracies tend to limit it to wartime activity.

As we move forward with the new realities of a digital world, information will not only be critical to, but also the key to, success in all domains. Furthermore, the exponential growth of technology and its widespread use has ensured that those who take part in information war are individuals, and not just armed forces. Advanced technology such as deep fakes, artificial intelligence, and 5G network speed will further refine cyber-enabled psychological operations, having profound effects on information warfare in particular and allowing us to recognize its new role in offensive and defensive operations. Yet the speed by which we act is not yet sufficient, and is instead reactive and inductive. Certainly, this is not to downplay the complexity of dealing with new types of warfare. In the real world, resources are often stretched and responses to adversarial behavior will probably always err on the side of being reactive rather than proactive. What matters most is that when we see these developments unfolding, we create the proper frameworks for addressing each individual problem area. Doing so will ensure the continuation of proper attention and resources being dedicated to combating new threats as they arise.

Disclaimer

The views presented in this article are those of the authors and do not necessarily represent the views of USSTRATCOM, the US Air Force, the DoD, or the US Government.

Acknowledgements

Thanks to Brian Burke and Tommy Nimrod, for their thoughtful expertise in regards to the information environment and psychology, respectively, in guiding this research.

Bethany Vailliant is an Analyst at the United States Department of Defense. She is also an Adjunct Professor teaching International Relations at the University of Nebraska at Omaha, where she earned her M.S. in Political Science with a certification in Intelligence and National Security.

bethanyrvailliant@gmail.com

Media Ajir is an Analyst at the United States Department of Defense. She is also an Adjunct Professor at the University of Nebraska at Omaha and Bellevue University, where she teaches International Relations and Political Science. She holds an M.S. in Political Science with a certificate in Intelligence and National Security.

majir@unomaha.edu

References

Adams, Tim. 2018. "The Charge of the Chadbots: How Do You Tell Who' Human Online?" *The Guardian,* November 18, 2018.

Ajir, Media and Bethany Vailliant. 2018. "Russian Information Warfare: Implications for Deterrence Theory." *Strategic Studies Quarterly* 12 (3): 70–89.

Allen, Patrick and Dennis Gilbert. 2018. "The Information Sphere Domain Increasing Understanding and Cooperation." NATO CCDCOE.

Banach, Stephan J. 2018. "Virtual War – A revolution in Human Affairs." *Small Wars Journal*

Bergal, Jenni. 2017. "Hacktivists Launch more Cyberattacks against Local, State Governments." *PBS.*

Brazzoli, M.S. 2007. "Future Prospects of Information Warfare and Particularly Psychological Operation: South African Army Vision 2020." *Institute for Security Studies, Pretoria*, 217–32.

Greenberg, Andy. 2019. "The WIRED Guide to Cyberwar." WIRED. August 23, 2019.

Heftye, Erik. 2017. "Multi-Domain Confusion: All Domains Are Not Created Equal." The Strategy Bridge. May 26, 2017.

Horning, Donna. 2011. "Cyberwar: The Fifth Domain of Warfare." The Politic. December 19, 2011.

Hwang, Tim, and Lea Rosen. 2017. "Harder, Better, Faster, Stronger: International Law and the Future of Online PsyOps."

Joint Chiefs of Staff. 2014. "Joint Publication 3-13. Information Operations."

Joint Chiefs of Staff. 2019. "Joint Publication 6-0: Joint Communications System."

Kagan, Frederick, Nataliya Bugayova, and Jennifer Cafarella. 2019. "Confronting the Russian Challenge: A New Approach for the U.S." Institute for the Study of War.

Kahneman, Daniel. 2011. *Thinking, Fast and Slow*. Farrar, Straus and Giroux.

Kovacich, Gerald, and Andy Jones. 2006. "High-Technology Crime Miscreants: Profiles, Motives, and Philosophies." In *High-Technology Crime Investigator's Handbook: Establishing and Managing a High-Technology Crime Prevention Program*, 2nd ed., 23–48. Elsevier.

Lin, Herb. 2020. "On the Integration of Psychological Operations with Cyber Operations." *Lawfare*. January 9, 2020.

Lin, Herbert. 2019. "The Existential Threat from Cyber-Enabled Information Warfare." *Bulletin of the Atomic Scientists* 75 (4): 187–96.

Marantz, Andrew. 2019. "The Dark Side of Techno-Utopianism." *The New Yorker*, September 23, 2019.

Patterson, Dan. 2018. "How Campaigns Use Big Data Tools to Micro-Target Voters." *CBS News,* November 6, 2018.

Raderstorf, Ben and Michael Camilleri. 2019. "Online Disinformation in the United States: Implications for Latin America." *The Dialogue.*

RAND. n.d. "Cyber Warfare." https://www.rand.org/topics/cyber-warfare.html.

Schmitt, Michael N., ed..2009. *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence.* Tallinn, Estonia: International Group of Experts.

Schreier, Fred. 2015. "On Cyber Warfare." Geneva Centre for Security Sector Governance.

Shallcross, N.J. 2017. "Social Media and Information Operations in the 21st Century." *Journal of Information Warfare* 16 (1): 1–10.

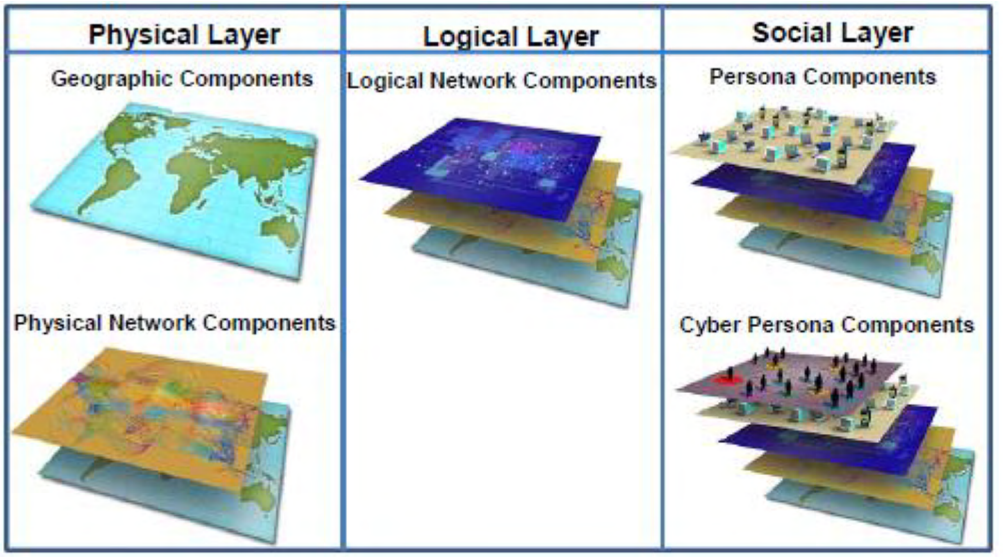
Shires, James. 2018. "Hack-and-Leak Operations: Intrusion and Influence in the Gulf." *Journal of Cyber Policy* 4 (2): 235–56.

Telley, Chris. 2018. "Influence at Machine Speed: The Coming of AI-Powered Propaganda." *Mad Scientist Laboratory*, May 24, 2018.

US Army. 2010. "Cyberspace Operations Concept Capability Plan 2016-2028." *The US Training and Doctrine Command, Fort Eustis*.

Wilmer, H.H., L.E. Sherman, and J.M. Chein. 2017. "Smartphones and Cognition: A Review of Research Exploring the Links Between Mobile Technology Habits and Cognitive Functioning." *Frontiers in Psychology* 8: 605.

Appendix 1



US Army, Cyberspace Operations Concept Capability Plan 2016-2028.

Psychology as a Warfighting Domain

Sarah Soffer*, Carter Matherly, and Robert Stelmack

Abstract

Using psychology to gain advantage over an enemy is as old as warfare itself. Psychological warfare predates its modern moniker, and military leaders have sought to understand their enemies and influence their behavior since military leaders emerged. In this paper, the authors discuss the history of psychology as a warfighting domain, using examples from myth and antiquity as well as select periods in which the United States or other countries used psychology to engage in conflict. An exploration of Russia's use of influence and its effect on the US highlight what conflict in the information environment looks like. The authors then briefly discuss the current state of information warfare and provide thoughts on what this will look like moving forward in an interconnected world.

Keywords: psychological operations, influence operations, information warfare, psychology, information operations, sixth domain, psychological domain

La psicología como dominio de guerra

Resumen

Usar la psicología para obtener ventaja sobre un enemigo es tan antiguo como la guerra misma. La guerra psicológica es anterior a su apodo moderno, y los líderes militares han tratado de comprender a sus enemigos e influir en su comportamiento desde que surgieron los líderes militares. En este artículo, los autores discutirán la historia de la psicología como un dominio de guerra usando ejemplos del mito y la antigüedad, así como períodos seleccionados en los que los Estados Unidos u otros países utilizaron la psicología para entrar en conflicto. Una exploración del uso de la influencia de Rusia y su efecto en los Estados Unidos resaltará cómo se ve el conflicto en el entorno de la información. Luego, los autores discutirán brevemente el estado actual de la guerra de información y ofrecerán ideas sobre cómo se verá avanzar en un mundo interconectado.

* Corresponding author: sjsoffer@gmail.com

doi: 10.18278/gsis.5.1.3

Palabras clave: operaciones psicológicas, operaciones de influencia, guerra de información, psicología, operaciones de información, sexto dominio, dominio psicológico

心理学作为一个战争领域

摘要

运用心理学来获得优势对抗敌人，这从战争起便存在。心理战的起源早于这一现代称呼，并且军事领导人从一开始便试图理解敌人，并影响后者的行为。本文中，作者使用传闻和古代事件实例，将心理学作为一个战争领域的历史进行探讨，并选择特定时间阶段，其间美国或其他国家使用过心理学参与战争。就俄罗斯使用影响力及其对美国造成的影响进行探究，将强调信息环境下的战争是什么。作者随后将简要探讨当前的信息战状态，并就信息战未来在互联世界中如何发展提供见解。

关键词：心理操作，影响力操作，信息战，心理学，信息操作，第六领域，心理领域

Introduction

While there are many Sun Tzu quotes touting the importance of psychology in war, one quote highlights the benefits of using psychology prior to and during war: "One need not destroy one's enemy. One need only destroy his willingness to engage" (Nylan 2020). Destroying the enemy's willingness to engage can take several forms: from causing the enemy to defect to convincing them to avoid engaging in the first place. In order to convince the enemy to avoid or cease engagement, one needs to understand how the enemy thinks: their motivations, background, fears, and culture. The purpose of this paper is to provide an overview of how psychology has always been part of large-scale conflict using examples throughout history. By providing these examples, the authors intend to emphasize the importance of a focused effort of utilizing psychology as a warfighting domain moving forward.

In order to examine the role of psychology as a warfighting domain, the authors define the terminology used throughout this paper. The authors then discuss examples of psychological warfare from ancient history and mythology. Then the authors then explore case studies chronologically

from different time periods during which the United States, US allies, and US adversaries have all used psychology—whether in the form of trickery and deceit to support other operations, messaging, or otherwise influencing how or what people think—to gain an advantage. After this broad overview of psychological warfare throughout time, the authors describe their opinions on the current state of influence operations and suggest a way forward.

To understand psychological warfare, one first must understand the terminology used to describe the various ways that militaries have used and continue to use psychology in war. According to the Department of Defense (DOD), psychological operations (PSYOP) "convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals" (DOD 2010). In recent years, the US Army rebranded PSYOP as Military Information Support Operations, or MISO—and then rebranded MISO back as PSYOP. Perhaps the easiest way to understand this shift is that MISO is what PSYOP does. MISO describes a broader range of operations, particularly when referring to operations involving the State Department (Myers 2017). Audiences consider MISO a less antagonistic term than PSYOP. The authors refer to PSYOP when discussing historic operations to keep consistency with the source material, but use MISO when the source material does as well. Military deception (MILDEC) is another way one uses knowledge of the adversary's thinking to achieve effects. MILDEC is used to "deter hostile actions, increase the success of friendly defensive actions, or to improve the success of any potential friendly offensive action" (DOD 2012). PSYOP/MISO and MILDEC (along with operations security, or OPSEC) fall under the general umbrella of Information Operations (IO). IO is defined in joint doctrine as the "integrated employment, during military operations, of information related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own" (DOD 2012). IO incorporates the ways to use the physical and information domains to influence the cognitive domain, which influences the physical and information domains in return.

Throwing Cats: Historical and Mythological Examples

Psychological warfare is not new to human conflict. Throughout history, people have used deception, disinformation, and influence over the decision-making of adversaries in warfare. Genghis Khan used techniques designed to inspire fear, the Egyptians had their cultural and religious beliefs used against them, and the myth of the Trojan Horse shows how powerful the idea of deception has been throughout human history. These three examples demonstrate how psychological warfare was used before "psychology" was a defined construct.

Genghis Khan is known as the man who conquered more land than anyone else in history. Part of his overwhelming success can be attributed to his ability to utilize psychological tactics in order to gain advantage over his adversaries. When Genghis Khan set his sights on a new territory, he offered sovereign leaders the opportunity to surrender and to meet all of his demands for tributes. If the other territory refused to give in, the Mongol armies slaughtered the majority of the population and only left behind a few storytellers, with the intent of having them tell this tale of terror to neighboring regions (Al-Khatib 2015). The message sent by these actions was for sovereign leaders to comply or face a horrific fate. This served to build up Genghis Khan's reputation, likely leading to him being able to conquer more territory without bloodshed than he otherwise would have been able to conquer. Without his ability to understand and manipulate the human psyche, Genghis Khan would have had to spend more time and resources in battle, rather than having leaders surrender without a fight.

Psychological warfare practitioners understand the importance of a target audience analysis, which is a study of a specific population that practitioners conduct in order to determine the best way to change a behavior. Cambyses II, leader of the Persian Army in the battle of Pelusium, 525 BCE, demonstrated the idea of understanding culture in order to evoke a specific response. The ancient Egyptians considered cats to be sacred, and even worshipped a goddess with the head of a cat: Bastet. The Egyptians viewed cats as Bastet's representation, and it was against the law for citizens to kill cats. Cambyses II had his soldiers capture as many cats as possible, and his troops gathered to try to take the city of Pelusium. Once the Egyptians attacked, the Persian Army released cats onto the battlefield. However, the confusion this induced was not enough for Cambyses II, who ordered the Persian soldiers to advance while they held cats or had them tied to their shields. The Egyptians, already confused and concerned because of the cats running everywhere, were afraid to shoot arrows at the enemy for fear of killing the cats and angering Bastet. The Persian army hurled cats over the wall of the city, inducing panic and confusion in the civilian population as well. Lastly, upon taking the city, Cambyses II kept a cage of cats and threw them in the faces of his enemies, showing his contempt and hatred for his enemies (Rouse n.d.). While Cambyses II may have won this battle even without this exploitation of Egyptian beliefs, his knowledge of Egyptian culture and religion certainly helped enable his victory in the battle of Pelusium. This highlights how understanding a population's culture and motivations can lead to success on the battlefield.

MILDEC is another method that militaries use that involves understanding the minds of the adversary. One example of this in antiquity is the tale of the Trojan Horse. While the tale of the Trojan Horse is likely more myth than reality, it is a classic example of using deception in warfare. This tale, described in Homer's *Iliad*, involves a frustrated

Odysseus seeking a way to get past the impenetrable walls of Troy. Supposedly inspired by the Greek goddess, Athena, Odysseus ordered a ruse in which all of the Greek army would appear to sail away and leave the gift of a large wooden horse for the city of Troy. The Greek army left one soldier, Sinon, behind to tell the Trojans how the Greeks had given up and left, with the horse as a gift. In reality, the Greeks hid their forces off the coast of a nearby island, with a small contingent of fighters left hidden inside the horse. The soldiers waited for the Trojans to enjoy a drunken celebration of their victory before they emerged from the horse to attack Troy from within (Cartwright 2018). This classic tale of deceit shows the importance of knowing the adversary's worldviews, their susceptibility to deception, and using multiple indicators to create a believable story. In this case, the Trojans' ego and hope for an end to the fighting perhaps allowed them to overlook the obvious strangeness of a large wooden horse left outside their gates. Because the army appeared to retreat, leaving one of their own behind to explain, the Trojans were more susceptible to believe what they wanted to believe—a psychological phenomenon now called confirmation bias.

These examples of evoking fear, understanding a target audience, and MILDEC demonstrate the use of psychological warfare in ancient times. While stories and myths from antiquity provide an entertaining glimpse of psychology as a warfighting domain, the rest of this article focuses on modern military and political efforts. Various time periods of conflict are discussed, using examples of different types of influence in order to highlight the importance of understanding and using human psychology to achieve effects in conflict.

"I Want You!" Posters and Propaganda during World War I

The world began to understand the utility of the psychological domain during World War I (WWI). One reason WWI is significant to the consideration of the psychological domain is its unique positioning in human history. This was the first time when the majority of nations involved in a conflict had well-educated, wealthy, and urbanized populations. Warfare was beginning to evolve and look different. There was another war behind the scenes of mechanized and trench warfare that characterized many of the battles. In this other war, governments fought to shape the opinions of the masses and to shape the ideas surrounding the war effort (Kaminski 2014). The US government began to understand the importance of propaganda—the spreading of ideas, information, or rumors for the purpose of helping or injuring an institution, a cause, or a person (*Merriam-Webster*, s.v. "propaganda," accessed January 18, 2020, https://www.merriam-webster.com/dictionary/propaganda)—propaganda, or the use of information (both true and false) to bolster the war effort. The goals of propaganda were simple; increase support for the war effort, boost military conscription, and lead

a war-making economy in the home front. Posters were the most widely used form of propaganda. The economies of the global powers facilitated mass production of propaganda efforts and allowed propagandists to develop advanced means of persuasion through an understanding of the human psyche.

Psychological theories, although not formally postulated at the time, allowed propagandists to use emotionally based methods that capitalized on patriotism, nationalism, and fear motivators (Chambers 1983). Social identity theory refers to the way in which a person's sense of who they are is based on group membership. Tajfel (1970) proposes that the groups to which people belong are an important source of pride and self-esteem and lead to dividing the world into "us" and "them" through social categorization. Terror management theory refers to the way that people respond to an awareness and fear of death (Greenberg, Pyszczynski, and Solomon 1986). This fear drives people to attempt to confirm their own sense of importance in the world and insulate themselves as a protective measure. These theories were used in propaganda efforts in the United States to influence the American public.

The United States distributed artistic propaganda predominantly using newspapers, leaflets, film, radio broadcasts, and large, colorful posters (Reed 2014). Much of the propaganda sought to increase support for the war effort by instilling American pride, increasing the "us" versus "them" divide, and by playing on people's fears. The messages contained within these mediums reached saturation in their target populations who internalized the messages as culturally definable and identifiable attributes. The messages were rooted in some kernel of information or cultural ideals upon which the larger message was built (Kaminski 2014). The US populace internalized the messages contained in the propaganda, which led to the messages becoming self-replicating – the more people were exposed to these ideas, the more they shared them person-to-person.

These messages were so internalized that they are still a part of American history and culture today. One of the most iconic pieces of Americana came from WWI propaganda. The ubiquitous Uncle Sam "I want YOU for the US Army" poster was, and still is, a compelling image to support one's nation. This demonstrates the principles of social identity theory by increasing people's ties to their group. Other posters encouraged those who could not join the military to support the war effort through work, savings, bonds, and even farming initiatives. In contrast to the general themes seen in US propaganda, German posters often conveyed an idea of national survival against an impending doom (Kaminski 2014). This demonstrates the use of terror management theory.

Another use of social identity theory involved emphasizing the division between US and adversarial populations. While much of the propaganda tended to appeal to traditional ideals of masculine and feminine protectorship roles, propaganda campaigns carried polarizing racial underpinnings (Olund

2017). Exaggerated ethnic features and portrayals of the "Hun" as large gorillas assisted observers in distancing themselves from the "other." Such imagery worked to create artificial psychopathy in the mind of the observer, allowing US troops to visualize the enemy as subhuman and therefore easier to attack. The use of this psychological tactic would grow darker in the coming decades.

US propaganda efforts toward its own citizens were very successful during WWI, both at home and abroad. The messages were so successful that, once World War II (WWII) began in earnest, the United States rebranded much of the material from WWI with images of new leadership (Kaminski 2014). The US use of propaganda to garner support from its own citizens while dehumanizing the enemy demonstrated how influence campaigns on the home front could support more traditional warfare.

Hitler in a Tutu: Weaponized Disinformation in World War II

During WWII, psychology served as a warfighting domain in several ways. While the US continued its influence campaigns at home, there was also a targeted use of psychological warfare against the adversary. Messaging in the form of leaflets, broadcasts, and other means served to lower the morale of enemy troops and increase their fear and confusion. Messaging took the form of white, gray, and black propaganda. White propaganda did not hide its source, gray propaganda obscured its source, and black propaganda appeared to come from another source, specifically from the person or group it was designed to discredit. In addition to lowering morale, messaging served to discredit the opposition and encouraged people to lose faith in the Axis powers. Disinformation campaigns bolstered MILDEC efforts with supporting actions, false armies, and false equipment. While both sides sought to dishearten, mislead, and weaken the other, the following examples focus on the efforts of US and Allied forces.

The US continued the tactics used in WWI to garner support among the US public. In order to do so, the United States created the Office of War Information (OWI) about half a year into its involvement in WWII. The purpose of the OWI was to produce white propaganda—messages from the US government targeting people at home and abroad with print, radio, film, and posters (Prosser and Friedman 2008). These posters encouraged Americans to refrain from sharing sensitive military information. Additionally, they encouraged Americans to do things such as walking instead of driving in order to help the war effort. The OWI created products that were innocuous in nature, but the US had another office to transmit black propaganda targeting the adversary—the Office of Strategic Services, or OSS.

The OSS's propaganda was one method the Allies used to try to lower enemy morale. They targeted this propaganda toward the enemy, masking the attribution of the messages. For example, Operation Cornflakes dropped mailbags full of fake newspapers into

Germany. These papers, appearing to be from Nazi resisters, worked to discredit Hitler. The OSS also used radio broadcasts that appeared to come from within Germany in order to convince the enemy that they had more resistance within the country than they expected (Little 2016). One branch, the Morale Operations (MO) branch, headed up most of the undercover propaganda campaigns with the intent of inducing fear, confusion, and distrust among the enemy. The MO and their British equivalent, the Political Warfare Executive, distributed rumors by word of mouth, radio broadcasts, and leaflets. Some of these rumors stated, "high-level Nazi leaders had been captured or had surrendered to the Allies" (Central Intelligence Agency [CIA] 2010). They also sent anonymous letters, called "poison-pen letters," to the families of German soldiers. These letters consisted of both death notices and letters describing how the soldiers died due to shoddy doctors. The letters intended to cause families to hate their own side, believing them incompetent.

Another method to erode support for the adversary involved the use of doctored photos. Back before Photoshopped images online called into question whether something was "fake news," the OSS suggested distributing postcards of Hitler that would make him an object of ridicule. The OSS proposed ideas like Hitler dressed as a male ballet dancer, Hitler dancing with children, and Hitler dancing with an obese woman (Friedman 2003). The purposes behind ridiculing the enemy are to raise morale back home, strip the enemy of mystique/prestige, erode the enemy's claim to justice, and reduce the idea of the enemy as invincible; depending on the culture, ridicule can be seen as a fate worse than death (Waller 2006). The OSS sought to undermine Hitler's efforts by weakening his support among the population.

In addition to spreading fear, confusion, and distrust, the Allied forces also engaged in MILDEC activities such as Operation Mincemeat. Operation Mincemeat is one of the well-known MILDECs from WWII and it highlighted how one must understand the adversary in order to fool them. When the Allies planned to invade Italy via Sicily, they were concerned that this was too obvious of a plan and that Germany and Italy would be able to anticipate and counter their efforts. In order to create a path of less resistance, the Allies created a disinformation campaign that led to the German forces believing the invasion would come from further east. The Allies accomplished this with a dead "military officer" planted where Axis forces could find the body. On the "officer's" body was false identifying documents and paperwork implicating an Allied invasion occurring at the false location. The Germans and Italians fell for the plan, allowing for a safer invasion of Sicily (Knighton 2017). This plan involved knowing which populations would be sympathetic to the Axis forces, the susceptibility of the enemy to believing the source documents, and a lack of contradicting information. A more suspicious adversary may not have fallen for this clever trick. Much like the use of the Trojan Horse, Opera-

tion Mincemeat used confirmation bias to manipulate the beliefs of the Italians and the Germans to pave the way for a successful invasion.

WWII demonstrated that a concerted propaganda effort could enhance military and political effectiveness. By attacking the enemy's feelings and emotions, it reduced their problem-solving capability, lured them into a false sense of security, increased fear, and lowered morale. Eroding support for adversary leadership led to a more permissive environment within which the Allied forces could operate. Between leaflet bombs, planted evidence, and departments specifically designed for different psychological tactics—OWI for improving morale and shaping behavior at home and OSS for reducing morale and shaping behavior amongst the enemy—WWII demonstrated the power of psychology in war.

Deception, Intrigue, and Math? Soviet Information Operations during the Cold War

The Cold War, much like WWII, was a breeding ground for propaganda, disinformation techniques, and psychological warfare methods used by both sides. President Truman kicked off a national "Campaign of Truth" in order to counteract Soviet propaganda. The goal of this campaign was to counter disinformation through "honest information about freedom and democracy" (Wolfe 2018). While the United States committed to truth as a method of psychological warfare (in addition to an increased focus on psychological warfare), the Soviet Union used other methods in order to try to gain an advantage over the US. Of particular note was their development, refinement, and execution of reflexive control theory (RCT).

Reflexive control is "a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action" (Kamphuis 2018). RCT stipulates that when two adversaries engage in conflict, the adversary who better understands their opponent's decision-making process and utilizes it against them is more likely to succeed. The increased probability of success follows a recursive algorithm. For example, if opponent A anticipates opponent B's decision-making process, opponent A is more likely to succeed. If opponent B anticipates that opponent A will be taking into account opponent B's decision-making process, opponent B would then have the advantage, and so on and so forth, with the final advantage being heavily influence by which opponent has the most accurate knowledge and is most successful at utilizing this knowledge of the other's decision-making process. The final desired outcome of successful reflexive control is to hijack the adversary's decision-making process so that they *reflexively* take decisions that advantage the RCT enabler.

In order to truly understand RCT, one must first understand its beginnings in *Maskirovka*, a concept within Russian strategic thinking defined as "deliberately misleading the opponent with regard to one's own in-

tentions, causing the opponent to make wrong decisions and thereby playing into one's own hand" (Kamphuis 2018). Essentially, *Maskirovka* is an art of deception and psychological manipulation. Russia applied *Maskirovka* on a large scale and immediately utilized it against the United States following the end of WWII. Russia sought to control the way the United States perceived Soviet nuclear development capabilities and allowed for the beginning of the nuclear arms race (Ziegler 2008). In summary, understanding *Maskirovka* is integral for understanding how Soviet doctrine incorporates deception and an understanding of their adversary's perceptions.

How does *Maskirovka* fit into RCT? While *Maskirovka* on its own is the integrated concept of deception, RCT is more than "controlling the perceptions of adversaries"—it is the process to control their decision-making process. Deception is just one piece of the overall puzzle. RCT was founded by Vladimir Lefebvre, who, in his own words, believed the concept of disinformation in military doctrine "seemed to me too narrow, because the important thing is not so much cheating an enemy as controlling his decision-making, and to conduct reflexive control, we have to start with constructing an enemy's model" (Murphy 2018). Clearly, Lefebvre's formulation of RCT theory required extensive understanding of its intended victims, and the USSR did just that. In 1982, James Phillips, a senior research at the Heritage Foundation, wrote an exposé on the Institute for US and Canadian studies, a Soviet-based organization that purported to be akin to the typical independent, US, Washington-based think-tank. The true story was much more sinister. Far from being an academic institution dedicated to the furthering of cultural research for the sake of academia, the Institute primarily took direction from the Committee of the Communist Party of the USSR and, more specifically, their International Affairs department. This institute, rife with connections to the Soviet Politburo, Soviet academia, and the GRU, provided an excellent center of information to enable true usage of RCT (Phillips 1982).

Russia further applied RCT in a concrete example at the height of the Cold War. During a military parade and international show of force, the Soviets went out of their way to place deliberate indicators among the show for Western military attachés and other intelligence collecting assets to observe. In particular, the Soviets manufactured multiple fake, larger intercontinental ballistic missiles (ICBMs) that appeared to support longer than currently believed maximum ranges and the capability of employing multiple warheads per ICBM. Using the tenets of RCT, Soviet planners did this with the understanding that the gathered intelligence would then make its way back to Western decision-makers and lead them to decide upon further intelligence gathering. "Getting into the heads" of said decision-makers, the Soviets had already created multiple collateral intelligence trails which would be picked up in other intelligence avenues and corroborate deliberately intended conclusions

(Thomas 2004). In this case, understanding the psychological characteristics of US decision-makers allowed Russia to compete with the US through psychological manipulation.

The Cold War was a fertile environment for the germination of non-traditional warfare means. Two superpowers were placed head-to-head in a battle for supremacy without the ability to rely on traditional schools of thought for international relations and military strategy. Both sides began to replace air superiority and decisive battles with espionage and proxy war. Beginning with their development of *Maskirovka* in turn of the twentieth century, the Soviet Union was well positioned to develop RCT, a mathematical, cybernetics-based solution to controlling their adversaries' decision-making abilities. This new approach to vying for supremacy, combined with the intense, specific research of the Institute for US and Canadian Studies, allowed for the refinement needed to enable RCT. The Soviet Union could effectively use RCT to hijack the Observe, Orient, Decide, and Act (OODA) loop, created in the fifties and typically used widely by the US military to describe decision-making. By understanding how a target orients and decides, RCT allowed the Soviet Union to predict behavior and insert a counter to create a "reorientation." There is present and significant evidence that the Soviet Union was able to master a new, innovative approach to grey-zone conflict and would have had no reason to abandon such a useful school of thought in recent years. The former Soviet Union has continued to influence US decision-making through psychological warfare in recent years, which the authors explore further on in this article.

Ghosts and Grievances in the Vietnam War

The Vietnam War was another period of conflict in which the US and other nations sought to amplify their effectiveness through psychological means. One example of this is reminiscent of how the Egyptian's beliefs were used against them. In Vietnam in 1967, there was a widely held Buddhist belief that spirits of the dead uneasily walked the Earth unless their relatives buried them properly. The primarily Buddhist North Vietnamese and the Viet Cong were dying far from home. These beliefs and facts led to the creation of Operation Wandering Soul. This operation was an effort by US soldiers to lower enemy morale and create fear and confusion (Hoyt 2017). The Sixth Psychological Operations Battalion (Sixth PSYOP) paired with the US Navy to broadcast audio consisting of Buddhist funeral music, unearthly sounds, and distressed voices of "ghosts" speaking of how they were now in Hell, wandering the Earth (Shirley 2012). While the United States used audio as a ruse previously in WWII during the "Ghost Army" recordings, the use of audio during the Vietnam War served as a way to take advantage of cultural and religious beliefs that the dead will wander the world looking for their bodies unless properly buried. The US was not solely responsible for this

effort—they relied on the South Vietnamese to be more effective.

The South Vietnamese helped the US transmit the haunting audio. Soldiers and helicopters both carried loudspeakers in order to create the perception that the haunting sounds were coming from multiple locations within the jungle. The audio failed to fool some soldiers but appeared to unsettle other soldiers. Even if enemy soldiers knew the sounds were false, they still reminded them that if they die, their souls could end up wandering the jungles in a similar fashion. Any moments of confusion or fear that the US could gain through Operation Wandering Soul was useful. The Sixth PSYOP even modified the audio to bolster the South Vietnamese rumor of a tiger attacking the North Vietnamese Army and Viet Cong troops. The Sixth PSYOP included tiger growls on the audiotape, and people reported that 150 men fled Nui Ba Den Mountain where the audio with tiger sounds was played (Friedman n.d.). While the US and South Vietnam played on the enemy's belief system to cause fear and confusion, other efforts focused on garnering support. One way they did this was through counterinsurgency efforts.

The South Vietnamese created a counterinsurgency program called Phuong Hoang—named after a mythological bird from Vietnamese and Chinese culture—while US officials in Vietnam called their supporting efforts the Phoenix program (Miller 2017). One influential figure, a South Vietnamese Army officer named Tran Ngoc Chau, demonstrated how effective efforts to "win hearts and minds" could be. Chau worked to counter insurgents in Kien Hoa. Kien Hoa was a difficult place to work because the government had difficulty identifying insurgents and villages were angry with local officials and police forces, which tended to be corrupt. Chau decided to conduct the Census-Grievance program to interview every adult in Kien Hoa, with the goal of collecting information about the enemy. While he was able to use these methods to track down enemies to have them captured, or killed as a last resort, one of the big wins of the Census-Grievance program was engaging the populace. By doing so, he showed that he listened to their complaints and responses, and then addressed the problems within his control. Chau did not approve of the Phoenix program's heavy use of force and lack of emphasis on mobilizing the population (Miller 2017). Instead, the lesson learned from the Census-Grievance program emphasized that understanding how and why people think led to an increased ability to gain population buy-in.

While the authors have discussed the role of deception and of understanding the populace, other efforts focused on increasing defectors among the Vietcong and the North Vietnamese Army. Operation Roundup on Kien Gieang targeted potential defectors by having defectors photographed and having them write messages on leaflets encouraging their former colleagues to defect and join the cause. Project Roundup also used loudspeaker teams of former Viet Cong soldiers to speak

to their former colleagues to convince them to defect. According to Colburn Lovett, a USIS Foreign Service officer, this led to hundreds of enemy defectors in the area. Similarly, Project Falling Leaves used armed teams of ex-Viet Cong members to deeply penetrate enemy territory in order to conduct face-to-face communications with Viet Cong soldiers. They also used loudspeaker teams, leaflet drops, radio, and television to spread ex-Viet Cong members' messages to defect (Goldstein and Findley 1996). By having former colleagues try to influence the Viet Cong and North Vietnamese army, the US sought to appeal to their emotions and once again appealed to people's sense of social identity.

The Vietnam War involved psychological methods of warfare from both sides. The Viet Cong and North Vietnamese Army relied heavily on fear tactics among their own people (Goldstein and Findley 1996), while the South Vietnamese and the United States influenced the enemy population using a blend of methods from traditional media, to loudspeakers, to face-to-face conversations. Some of these methods, such as Chau's Census-Grievance program and Operations Roundup and Falling Leaves allowed for fewer casualties while increasing the number of defectors. Psychological warfare took on a multi-pronged approach to attempt to achieve victory in Vietnam. There are many well-known lessons learned from the Vietnam War, but psychological warfare practitioners can also learn from this conflict, particularly how to engage populations during irregular warfare. The methods used to influence adversaries have continued to evolve from these more overt methods of psychological warfare to a more hidden and subtle approach.

A Fire Hose of Fake News: Disinformation in the Age of Information

Psychological warfare between world powers continues to evolve and be used today. During the 2016 US presidential elections, the American public started to become familiar with terms like "trolls," "bots," and "fake news." While Russia's technique of using active measures and RCT was not new, US society's move to the internet and social media as sources of information enabled new ways to use these methods. In 2015, Russia enacted their largest targeted hacking campaign in order to find compromising materials on US political leaders. They were able to access much of the information from the Democratic National Committee (DNC) servers, but the Republican National Committee (RNC) servers are postulated to have had less usable information due to migration to newer hardware (Watts 2019). Russia's attack on US democratic processes consisted of trolls, bots, cyber-attacks, and state-run propaganda efforts.

Russian trolls used a mixture of spreading disinformation and strategically timing their amplification of facts in order to cause the most chaos and distrust among the US populace. Trolls, coupled with the use of bots, allow Russia to disseminate a large amount of "in-

formation" through various channels in order to overwhelm people and reduce their ability to discern truth from lies. This method, called "the firehose of falsehood" (Paul and Matthews 2016), runs counter to traditional means of influence, which relies on trust, credibility, and message synchronization. During the months leading to the 2016 election, "the troll army began promoting candidate Donald Trump with increasing intensity, so much so their computational propaganda began to distort organic support for Trump, making his social media appeal appear larger than it truly was" (Watts 2019). Once polls started to indicate that Trump may not win, Russia focused on spreading the idea that voting machines were hacked and the election was compromised—a tactic that backfired on them when Trump won the election. Years later, the US still appears to be divided, with people's faith in elected leaders and democracy continuing to decrease.

Disinformation is spread through social bots, which amplify false claims, allowing them to go viral on websites like Twitter. This ties into the previously mentioned "firehose of falsehood" method because several different versions of a story can be widely shared until a wider audience picks it up and amplifies its message. Twitter estimated that there are 1.4 million Russian-linked accounts (Watts 2019), many of which are bots amplifying messages spread through trolls and state-sponsored propaganda. Bots can be used to spread information acquired through hacking. Twitter data provided to the US House of Representatives showed over 36,000 Russian-linked bot accounts tweeting about the US election, with 288 million Russian bot tweets, and over 130,00 tweets directly linked to Russia's Internet Research Agency (IRA) (US House of Representatives 2018).

Leading up to the 2016 election, Russia used multiple methods to instigate strife between Americans and to spread disinformation. Another method used was Facebook advertisements with over 3,500 IRA advertisements and 11.4 million Americans exposed to those advertisements and 470 IRA-owned Facebook pages with 80,000 pieces of content created by those pages and 126 million Americans exposed to that organic content (US House of Representatives 2018). These are startling numbers that show how effective the IRA has been in understanding and exploiting American culture. They not only spread disinformation, but also exploited people's emotions; for example, they encouraged people to believe that their votes did not matter so they should vote third party or forgo voting altogether (Thompson and Lapowsky 2018).

Russia's attempts at creating division, or schismogenesis, of the American public lead to questions on how to counter an information environment saturated with fake news. Overall, people are susceptible to the spread of disinformation, with 23 percent of adults sharing fake stories during the months leading up to the 2016 election (Anderson and Rainie 2017). Both older and younger generations are susceptible for different reasons, with older adults lack-

ing an understanding of the internet and of the threat of state actors, while overfamiliarity of the internet leads to younger generations' vulnerability. With younger adults growing up in a culture where information is readily available through Google searches and anyone online can appear to be an expert, it can be challenging to convince younger adults to analyze articles and their sources (Conger 2019). This manipulation of the American public has not ceased and combating the spread of misinformation and disinformation is one of the current struggles the influence operations community is facing today. It is crucial for the United States to find ways to counter disinformation in order to retain its status as a world power.

Information Warfare Today

The United States continues to explore how to shape the behaviors of decision-makers, from working to enhance a friendly nation's perception of the US, through strategic communication, to influencing adversaries either to avoid conflict or enhance ongoing war efforts. Modern advancements in technology and psychological theory have enabled nation-states to reach individuals in ways previously considered unimaginable. The fiscal cost once associated with creating and spreading information and disinformation is no longer as much of a consideration. As history shows, the IO arena and the ability to influence an individual's cognitive and implicit processes have only become more subversive and easier to produce. However, there are some obstacles preventing the United States from being as successful with messaging and countering disinformation as other countries.

The ease and impact of modern psychological operations have made their use extremely appealing to a multitude of nations. For example, Russia has worked diligently to unify its operations for the purposes of external influence. China has taken a different approach, leveraging introspective campaigns against its own citizens. North Korea has also embraced the psychological approach, sans technology, using cultural factors to influence its population (Matherly 2019). As the capabilities of these nations grow stronger, the United States lags further behind. Disjointed and poorly defined operations often create power vacuums or oversaturate the information environment, leading to mixed messaging and weak campaigns. The results are ineffective and create messaging that lacks the influence intended.

The United States is at risk of critically falling behind near-peer adversaries in the realm of IO. In a military system conceptualized around warfighting domains, the time has come to designate a new warfighting domain: the psychological domain. Doing so would allow the US to leverage capabilities like those of US adversaries. Leaders do not need to look far because pockets of excellence already exist within the DOD. These include US Army PSYOP command, the Marine Corps Information Operations Com-

mand, the Navy Information Warfare Systems Command, and the USAF's newly minted Information Operations Officer, or 14F, community, bolstered by the also new 16th Air Force, which was designated specifically as a centralized unit for information warfare. Unfortunately, what is currently lacking is a unity of command between these communities and confusion about the ownership of the messaging. These are only a start toward fully utilizing an operational understanding of to the psychological domain. While military leaders increasingly view information as a domain, they tend not to focus on the battle space fought in the cognitive realm, instead choosing to focus on non-kinetic effects, such as cyber and electronic warfare. As history has shown, the psychological domain is a strategic weapon with effects spanning all other domains and dissemination methods that rely on the same.

Psychological warfare also faces challenges based on the perception of the public and of decision-makers who choose whether or not to employ influence operations. In an arena where the theme is "perception is everything," influence operations are failing at perception management. With programs like MK Ultra, in which the CIA conducted mind control experiments on US citizens (*Project MK Ultra, the CIA's Program of Research in Behavioral Modification* 1977), the general population has reason to distrust the intentions of any type of psychological operation. With the abundance of misinformation and disinformation being spread online, people are often either overly critical of true information or only trust information confirming their preconceived biases. People often do not understand psychology, partially because the wealth of information available online has led to a population that believes that a layperson can be as informed as an expert (Nichols 2017). Online quizzes lead people to believe they understand personality tests, and therefore psychology as a whole. This perception may cause key decision-makers to forgo the use of psychological tactics in order to focus on traditional methods of warfare.

IO practitioners need to realize that the United States cannot and should not employ the psychological domain in the same reckless way that Russia does. The US aims to show the rest of the world that we are a proponent of trustworthiness and fairness. As a result, creating and distributing false stories would quickly erode the image of trustworthiness the US wishes to foster. Because the US values integrity, communicators delay releasing information in order to fact-check, a strategic weakness in the information arena, which leaves a void in which other countries can dominate the narrative with inflammatory and false headlines. In the world of fake news and intriguing headlines, what people see first often sticks, regardless of truth. If the US were to forgo a commitment to the truth, we would betray our cultural values, and the US would lose credibility in the eyes of the rest of the world (Watts 2019). Fortunately, often the best propaganda is true, so the US should continue to work to be a key leader in influence operations without betraying

US values. This may require creative and innovative solutions to these modern phrases, so exploring new means to share messages while countering disinformation campaigns is critical.

The psychological domain represents the next great shift in warfare. Other nations are choosing to leverage the domain in a way to propagate falsehoods and sow global divisiveness. The US has long stood as a stalwart of truth in rhetoric, often delivering stale and late timed facts to a conversation. By the time the facts have been delivered, fake stories have already convinced the public. If the US is to regain its footing, the DOD should not only formalize a sixth warfighting domain, but should also act to seize the narrative. As history has shown during major combat operations, the DOD has successfully leveraged this capability. The main difference between the information sphere today and during WWII or the Cold War is ease of access. The modern threat, danger, and risk of failure in the information environment are real, and an emphasis on psychological approaches could help.

Future research would benefit from articulating a way forward for the DOD, including what command structures and authorities would look like. This article's review of past uses of psychology as a warfighting domain stresses the importance of such an endeavor. The case studies the authors highlighted show that understanding human psychology changes the ways nations conduct warfare. Information is a source of national power, but without a unified and clearly defined domain, there is no way to decisively dominate and yield this power. Within the domain of psychology rests the opportunity to see an end to conflict before it begins, as Sun Tzu argued centuries ago.

Psychological warfare has a varied but significant history and was used both as a tool for nations to take on their foes and as a method to inspire and influence their own populations. During the Classical Era, the Trojan Horse was infamously used as a deceptive device that would force capitulation upon the enemy. Fast-forward to the World Wars, and propaganda was successfully used both to inspire friendly populations and to deter adversary populations from participating in their war efforts. Methodology and psychological science developed during the global conflicts and onwards, within the Soviet Union in particular, led to the refinement of RCT, an operational level planning tool for IO, while the United States refined and developed tactics and equipment for tactical level employment of PSYOP and influence operations. IO continued its evolution into the modern age, where electronic warfare, cyber operations, and the third industrial revolution redefined information operations like never before due to the new speed with which people could generate, transmit, and ingest information. Despite significant changes in information management, the key tenets of IO, based on influencing people, have remained steadfast and will continue to do so as long as human nature remains the same.

Sarah Soffer holds an MS in Psychology from Missouri State University and an MS in Anthropology from Purdue University. Her research interests include the role of social media in influence activities as well as organizational support to veteran and military members. She currently serves as an Information Operations officer in the U.S. Air Force.

Carter Matherly holds a PhD in Psychology and an MS in Intelligence Analysis. His primary area of research includes the application of psychological principals to intelligence problem sets and advocacy for a psychological warfighting domain. Highlights from his research include identifying the psychological motivators for individuals who join terrorist organizations as well as dissecting North Korean propaganda. He welcomes opportunities for continued research and collaboration.

Robert Stelmack holds a BS in Political Science from the United States Air Force Academy. He is an Information Operations officer in the U.S. Air Force. His primary area of research is information and hybrid warfare, specifically focusing on the function of national identity.

References

Al-Khatib, Talal. 2015. "Hearts and Minds: History of Psychological Warfare." *Seeker*, April 29, 2015. https://www.seeker.com/hearts-and-minds-history-of-psychological-warfare-1769783167.html.

Anderson, Janna and Lee Rainie. 2017. "The Future of Truth and Misinformation Online." *Pew Research Center*. https://www.pewresearch.org/internet/2017/10/19/the-future-of-truth-and-misinformation-online/.

Cartwright, Mark. 2018. "Trojan War." *Ancient History Encyclopedia*, March 22, 2018. https://www.ancient.eu/Trojan_War/.

Central Intelligence Agency. 2010. "The Office of Strategic Services: Morale Operations Branch." https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/oss-morale-operations.html.

Chambers, R. 1983. "Art and Propaganda in an Age of War: The Role of Posters." *Scientia Militaria, South African Journal of Military Studies* 13 (4): 54–59.

Conger, J. Z. 2019. "The Future of Fake News." *Over the Horizon: Multi-Domain Operations & Strategy*, October. https://othjournal.com/2019/10/28/the-future-of-fake-news/.

Department of Defense. 2010. "Psychological Operations." *Joint Publication 3-13.2.* https://fas.org/irp/doddir/dod/jp3-13-2.pdf.

———. 2012a. "Information Operations." *Joint Publication 3-13.* https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.

———. 2012b. "Military Deception." *Joint Publication 3-13.4.* https://info.publicintelligence.net/JCS-MILDEC.pdf.

Friedman, Herbert. 2003. "The Vilification of Enemy Leadership in WWII." *PsyWarrior,* November 1, 2003. http://www.psywarrior.com/AxisLeadersMonsters.html.

———. n.d. "The 'Wandering Soul' Tape of Vietnam." *PsyWarrior.* Accessed January 11, 2020. http://www.psywarrior.com/wanderingsoul.html.

Greenberg, J., T. Pyszczynski, and S. Solomon. 1986. "The Causes and Consequences of a Need for Self-Esteem: A Terror Management Theory." In *Public Self and Private Self*, 189–212. Springer Series in Social Psychology. New York: Springer.

Goldstein, Frank, and Benjamin Findley. 1996. "US and Vietcong Psychological Operations in Vietnam." In *Psychological Operations: Principles and Case Studies*, 233–41. Air University. https://media.defense.gov/2017/Apr/07/2001728209/-1/-1/0/B_0018_GOLDSTEIN_FINDLEY_PSYCHLOGICAL_OPERATIONS.PDF.

Hoyt, Alia. 2017. "Ghost Tape No. 10: The Haunted Mixtape of the Vietnam War." *HowStuffWorks*, May 16, 2017. https://science.howstuffworks.com/ghost-tape-no-10-haunted-mixtape-the-vietnam-war.htm.

Kaminski, J. J. (2014). "World War I and Propaganda Poster Art: Comparing the United States and German Cases." *Epiphany. Journal of Transdisciplinary Studies* 2: 64–81.

Kamphuis, Christian. 2018. "Reflexive Control." *Militaire Spectator,* June 21, 2018. https://www.militairespectator.nl/thema/strategie-operaties/artikel/reflexive-control.

Knighton, Andrew. 2017. "Four Great Military Deceptions of World War Two." *War History Online*. February 23, 2017. https://www.warhistoryonline.com/world-war-ii/4-great-military-deceptions-world-war-two.html.

Little, Becky. 2016. "Inside America's Shocking WWII Propaganda Machine." *National Geographic*, December 19, 2016. https://www.nationalgeographic.com/news/2016/12/world-war-2-propaganda-history-books/#close.

Matherly, C. 2019. "Examining Attitude Functions of North Korean Cultural Propaganda." *North Korean Review* 15 (1): 94–108.

Miller, Edward. 2017. "Behind the Phoenix Program." *The New York Times*, December 29, 2017. https://www.nytimes.com/2017/12/29/opinion/behind-the-phoenix-program.html.

Murphy, Jack. 2018. "Russian Reflexive Control Is Subverting the American Political Landscape." *SoFrep*, September 26, 2018. https://sofrep.com/news/russian-reflexive-control-is-subverting-the-american-political-landscape/.

Myers, Megan. 2017. "The Army's Psychological Operations Community Is Getting Its Name Back." *ArmyTimes*, November 6, 2017. https://www.armytimes.com/news/your-army/2017/11/06/the-armys-psychological-operations-community-is-getting-its-name-back/.

Nihon Kessho Gakkaishi, 19 (Supplement). (1977). doi:10.5940/jcrsj.19.supplement_2c-5

Nylan, Michael. 2020. *The Art of War: A New Translation by Michael Nylan*. 1st ed. New York: W. W. Norton & Company.

Olund, E. 2017. "Multiple Racial Futures: Spatio-Temporalities of Race during World War I." *Environment and Planning D: Society and Space 35* (2): 281–98.

Paul, Christopher and Miriam Matthews. 2016. "The Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It." *The RAND Corporation*. https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf.

Phillips, James. 1982. "Unmasking Moscow's 'Institute of the USA.'" *Homeland Security.* https://www.heritage.org/homeland-security/report/unmasking-moscows-institute-the-usa.

Prosser, Frank and Herbert Friedman. 2008. "Organization of the United States Propaganda Effort during World War II." *Psywar.Org*, May 6, 2008. https://www.psywar.org/usa.php.

Reed, Stacey. 2014. "Victims or Vital: Contrasting Portrayals of Women in WWI British Propaganda." *Hohonu* 13: 81–92.

Rouse, Ed. n.d. "Psychological Operations/Warfare." *PsyWarrior*. Accessed January 18, 2020. http://www.psywarrior.com/psyhist.html.

Shirley, Robert. 2012. "Operation Wandering Soul (Ghost Tape Number 10)." *YouTube.* July 7, 2012. https://www.youtube.com/watch?v=4d9H_1ygEv8.

Tajfel, H. 1970. "Experiments in Intergroup Discrimination." *Scientific American* 223 (5): 96–103.

Thomas, Timothy. 2004. "Russia's Reflexive Control Theory and the Military." *Journal of Slavic Military Studies* 17: 237–56. doi:10.1080/13518040490450529.

Thompson, Nicholas and Issie Lapowsky. 2018. "How Russian Trolls Used Meme Warfare to Divide America." *Wired*, December 17, 2018. https://www.wired.com/story/russia-ira-propaganda-senate-report/.

US House of Representatives. 2018. "Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements." https://intelligence.house.gov/social-media-content/.

Waller, J. Michael. 2006. "Ridicule as a Weapon." White Paper 7. Public Diplomacy White Paper. *The Institution of World Politics.* https://www.iwp.edu/wp-content/uploads/2019/05/20060209_RidiculeasaWeapon2.2.1.pdf.

Watts, Clint. 2019. *Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News*. Harper Paperbacks.

The White House. 2017. "National Security Strategy of the United States of America." https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

Wolfe, Audra. 2018. "Project Troy: How Scientists Helped Refine Cold War Psychological Warfare." *The Atlantic*, December 1, 2018. https://www.theatlantic.com/science/archive/2018/12/project-troy-science-cold-war-psychological-warfare/576847/.

Ziegler, Charles. 2008. "Intelligence Assessments of Soviet Atomic Capability, 1945–1949: Myths, Monopolies and Maskirovka." *Intelligence and National Security* 12 (4): 1–24. doi:10.1080/02684529708432446.

Discovering Influence Operations on Twitch.tv: A Preliminary Coding Framework

Alexander Sferrella and Joseph Z. Conger

Abstract

Bots are an important tool for influence actors, and greatly contribute to the complexity and breadth of influence operations (IFOs) across many platforms. Twitch.tv—the second-most popular streaming site—is one such platform. Recognizing that influence actors may expand operations within Twitch, the following study develops a framework that mines data from the Twitch platform to identify potential bots running IFOs. Stream comments from 14 Twitch channels were run through a custom Python script. We identified 69 of 128 streams, from 12 channels, as having an anomalous comment count OR comment speed. Of those streams, we identified 7,332 users as having an anomalous comment count AND comment speed. However, we could not distinguish 100 randomly selected anomalous users as bots or humans after a manual analysis. Overall, our research provides future researchers with a modular method to collect and isolate Twitch data containing bots.

Keywords: influence operation, influence actor, social media, streaming, Twitch, bot, psychological domain, sixth domain

Descubriendo las operaciones de influencia en Twitch.tv: un marco preliminar de coding

Abstract

Los bots son una herramienta importante para los actores de influencia y contribuyen en gran medida a la complejidad y amplitud de las operaciones de influencia en muchas plataformas. Twitch.tv, el segundo sitio de transmisión más popular, es una de esas plataformas. Reconociendo que los actores de influencia pueden expandir las operaciones dentro de Twitch, el siguiente estudio desarrolla un marco que extrae datos de la plataforma Twitch para identificar posibles bots que ejecutan operaciones de influencia. Los comentarios de flujo de 14 canales de Twitch se ejecutaron a través de un script Python personalizado. Identificamos 69 de 128 transmisiones, de 12

 doi: 10.18278/gsis.5.1.4

canales, con un recuento de comentarios anómalos O una velocidad de comentario. De esas transmisiones, identificamos a 7.332 usuarios con un recuento de comentarios anómalos Y una velocidad de comentario. Sin embargo, no pudimos distinguir 100 usuarios anómalos seleccionados al azar como bots o humanos después de un análisis manual. En general, nuestra investigación proporciona a los futuros investigadores un método modular para recopilar y aislar los datos de Twitch que contienen bots.

Palabras clave: operación de influencia, actor de influencia, redes sociales, transmisión, Twitch, bot, dominio psicológico, sexto dominio

探究Twitch上的影响力操作：一项初期编码框架

摘要

网络机器人是影响力行为者的一项重要工具，它极大地促进了许多平台中影响力操作的复杂性和广度。Twitch.tv—第二大最受欢迎的流媒体网站—就是这样的平台。意识到影响力行为者可能在Twitch内扩大操作后，以下研究提出一项从Twitch平台挖掘数据的框架，以识别执行影响操作的潜在网络机器人。通过一个定制Python脚本程序分析了14个Twitch频道的实时流评论。我们从12个频道中的128个视频流中识别出69个带有异常评论数或评论速度的视频流。从这69个视频流中，我们识别出7332名用户的评论数及评论速度均为异常。然而，经过人工分析后，我们无法区别100个随机选择的异常用户是机器人还是真人。总体而言，我们的研究为未来研究者提供了一个用于收集和分离包括网络机器人的Twitch数据的模块化方法。

关键词：影响力操作，影响力行为者，社交媒体，流媒体，Twitch，网络机器人，心理领域，第六领域

Introduction

The purpose of this study is to develop and execute a data-mining algorithm that can identify bots on the Twitch.tv (Twitch) platform. Before we discuss the study, we first must examine what influence operations (IFOs), bots, and Twitch are.

IFOs are the "coordinated, integrated, and synchronized application of national diplomatic, informational,

military, economic, and other capabilities in peacetime, crisis, conflict, and post-conflict to foster attitudes, behaviors, or decisions by foreign target audiences that further [a country's] interests and objectives" (RAND 2009, xii). The advent of the internet magnified the ability and reach of individuals and organizations to coordinate IFOs. Given its low cost and high effectiveness, Internet-based IFOs have become a permanent addition to the peacetime and wartime toolkits of state and non-state actors (Collins 2018; FireEye Intelligence 2018; Insikt Group 2019; RAND 2016; Stanford Internet Observatory 2019; Twitter 2019; Zakrzewski 2019).

The introduction of bots— automated computer programs that execute preprogrammed instructions—makes IFO distribution even easier. These bots mimic human users and can interact with other users and computer systems, rapidly creating trends and disseminating messages (Prier 2017). As evidenced by the US 2016 election, bots can have far-reaching impacts on public opinion (Howard et al. 2018).

The combination of increased at-home use of the internet, the introduction of social media as a social connector and news aggregator, bot development, and increased interest in the effectiveness of IFOs by state and non-state actors has caused the exponential growth of disinformation and IFOs (Sander, 2019). In early 2006, approximately 53 percent of adults used the internet at home, and 10% used social media (NTIA 2018; Pew Research Center 2019); these numbers grew to 72 percent and 69 percent, respectively, by early 2018 (NTIA 2018; Pew Research Center 2019)—increasing internet availability has increased target audience volume.

Foreign powers are conducting IFOs on platforms used by younger people, such as Reddit and Instagram (Reddit 2019; Roose 2018). Among these platforms, Twitch.tv has risen in popularity. Twitch is an extremely popular streaming service, second only to Netflix and ranked the 30th most popular site in the world by Alexa's web rating (Iqbal 2019). Streamers on Twitch provide a live video feed that is viewed by users. It currently hosts 2.2 million daily broadcasters and 15 million daily users, and the platform's audience continues to grow (Iqbal 2019). Videogames are primarily streamed, but other categories—such as sports and politics—are popular as well. Users who create a profile are able to follow content creators, add friends, and discuss the live stream with other users. Users can communicate with the host streamer and other users through a chat window embedded on a stream's page (see Figure 1). The chat window is of a limited size, and will only show a maximum of 26 individual one-line comments. Stream chats tend to fall into three categories: empty streams, where no users comment in the chat; conversational streams, where users comment at a speed that allow for users to respond to each other and hold conversations; and rapid-posting streams, where users post so quickly that a given comment is displayed for mere seconds before being replaced by newer comments.

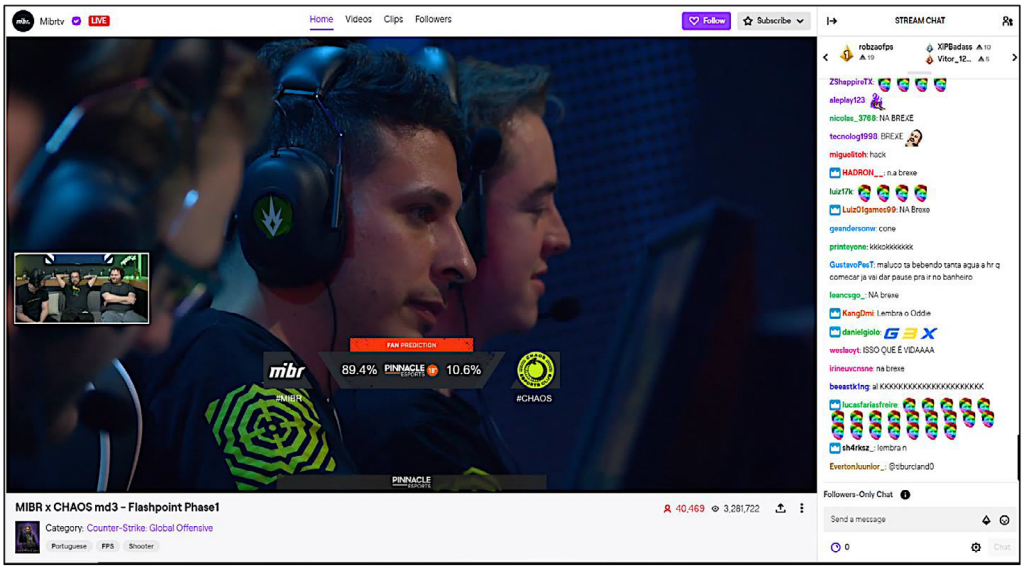


Figure 1: Example of Stream + Chat (Sample: Mibrtv, 3/14/2020).

To-date, no study has been conducted to discover IFOs on Twitch. We predicted that IFO actors would employs bots to achieve their objectives, so we built and executed a data-mining script in Python to identify users who post in a bot-like manner (defined in the methods). We further analyzed approximately 100 users who met our bot/bot-like criteria to determine whether or not they were actual bots supporting an IFO.

Methods

Previous researchers have built bot-detection programs utilizing multiple methods, such as decorate classification (Lee et al. 2010), Naïve Bayes (Wang 2010), Jrip (Ahmed and Abulaish 2013), Random Forest (Chu e. al. 2012), contrast patterns (Loyola-González et al. 2019), and Botometer (Yang et al. 2019). Because the Twitch platform includes a separate commenting interface from traditional social media sites, such as Facebook and Twitter, we coded a simple bot classification tool to serve as a starting place for more advanced bot researchers. But first, we make a number of assumptions about how an IFO might be conducted over Twitch:

1. IFO actors prefer to automate their operations.
2. Even if IFO actors have the resources to target *all* twitch streams, to do so would be overly conspicuous and therefore counterproductive.
3. IFO actors selectively target the streams they attempt to influence.
4. IFO actors do not target individuals on the platform, and instead target the largest number of users possible.
5. IFO actors do not target empty streams.

Table 1: January 29, 2020 Chat Log Download

Channel	Stream Type	Anomalous Streams	Total Streams	Anomalous Users	Total Users	% Anom. Users
bastiat	Political	6	10	83	2610	3.18
Bernie_Sanders	Political	0	10	0	3117	0
DemocracyLive	Political	6	10	28	1105	2.53
DonaldTrump	Political	0	5	0	9471	0
hasanabi	Political	7	10	2101	37994	5.53
skynews	Political	1	3	18	1294	1.39
touringnews	Political	1	10	5	670	0.75
washingtonpost	Political	9	10	748	14203	5.27
hutch	Political/ gaming	3	10	179	4378	4.09
JakenbakeLIVE	Political/ live blogging	10	10	2412	40269	5.99
Alinity	Live blogging/ gaming	10	10	486	13588	3.58
badbunny	Live blogging/ gaming	7	10	227	6952	3.27
ninja	Gaming	6	10	658	37628	1.75
riotgames	Gaming	3	10	387	13568	2.85
Total		**69**	**128**	**7332**	**186847**	

6. IFO actors target conversational streams with automated comments. If automated comments are engaged with, human actors can take over for manual commenting.

7. IFO actors target rapid-posting streams with short messages in a quantity-over-quality approach (e.g. spamming the hashtag "#FREE TIBET" in chat).

8. In conversational and rapid-posting streams, IFO actors post more than the stream's norm, as they are trying to make their comments stand out against the rest of the chat. By posting more frequently and/or in higher volumes, IFO actors' comments are identifiable via statistical techniques.

We selected 14 Twitch.tv channels for analysis, and included political or apolitical content creators (see Table 1). We handpicked channels to confirm proof of concept, rather than to execute a completely unbiased study. We chose popular channels because IFO actors likely want to target many users at once. We expected that political channels would have a greater bot

presence than non-political channels, as political channels generate more divisive discussions. Political channels included liberal, conservative, and neutral channels (e.g., Bernie Sanders', President Trump's, and the Washington Post's Twitch channels, respectively). To search for bots, we assumed that bot users post more comments and post at a higher rate than average users. We deemed streams that returned data indicating bot or bot-like user posting as "anomalous." The code used for this project is located at https://github.com/SferrellaA/twitch-analysis.

To prepare the dataset for analysis, the commentScraper.py script used the Twitch-Chat Downloader library (https://pypi.org/project/tcd/) to download the comments from the last 10 streams of Twitch channels listed in config.ini. The comments were downloaded in .srt (SubRip subTitle) files, which were then refactored into .csv (Comma-Separated Value) files with the commentRefactor.py script.

To analyze the downloaded chat logs, we ran the videoStats.py script. While analyzing an individual stream, the script did the following:

1. A data structure was created that associates a commenter's username with the number of comments they wrote. That is, by providing a given number, such as three, a list of all users that wrote three comments would be generated.

2. A data structure was generated that associates a commenter's username to their average and range of comment speed (in milliseconds). That is, by providing a username, that user's average and range of comment speed would be generated.

    a. Average comment speed was defined as the average number of milliseconds of all of the users' comments.

    b. Range of comment speed was defined as the difference between the longest and shortest time between the user's comments. To calculate this, only users with at least three comments were considered. Comment speed range was not used in this study, but could be used in future iterations.

3. The mean and median comment **count** of each stream was then calculated. Due to the nature of Twitch's platform, most streams have right-skewed count distributions. That is, most users write very few comments, and a few users write so many comments that they bring the stream's comment count mean above the median.

    a. Mean comment count was defined as the average number of comments posted by users. Users that only watched a stream but did not comment were not considered in the results.

    b. Median comment count was defined as the middlemost count of comments posted by users.

4. The mean and median comment

speed of each stream was then calculated.

   a. Mean comment speed was defined as the average of the users' comment speeds calculated earlier (only users with at least three comments).

   b. Median comment speed was defined as the middlemost of the users' comment speeds calculated earlier.

5. The stream was considered anomalous if users were commenting in greater volume and at greater speed than would be expected based upon the stream's median comment count and comment speed. For this study, a value of 3 was used to establish significance; that is, a mean comment count at least three times the median comment count, or a mean comment speed at most one-third the median comment speed (in milliseconds). This was a subjective definition and can be adjusted for future studies by editing the config.ini file.

6. The users of an anomalous stream were then reviewed. If exhibiting anomalous behavior of their own, their comments were recorded for review by a human reviewer.

   a. Anomalous users were defined as users whose individual comment count was at least three times the stream's median comment count and who had a mean comment speed at most one-third of the stream's median comment speed.

Results

The custom Python script analyzed 186,847 users across 128 streams from 14 Twitch channels. Of these, we found 7,332 anomalous users across 69 anomalous streams from 12 of the Twitch channels (see Table 1). An archive of the users and comments given in Table 1 is available upon request.

We randomly selected and manually reviewed 100 anomalous users, but none were clearly bots. These users posted comments of varying length and content, and many responded actively to other users, suggesting a human was commenting on the stream.

Discussion

Due to user volume, it was not feasible to manually review all identified anomalous users. The overwhelming majority of the manually reviewed anomalous users were engaged in mere chat spam (rapidly creating or copy-pasting inflammatory, humorous, or emoji comments). Surprisingly, neither the Donald Trump nor Bernie Sanders Twitch channels had anomalous users. We expected IFO actors to target voting-age users within these two channels as the 2020 election approaches, but the lack of IFOs may be explained by IFO actors' ignorance of the Twitch platform itself. Additionally, these two channels did not stream

often, which might be less appealing to IFO actors because there is no schedule for users and IFO actors to follow. In general, the highest percentages of anomalous users were from channels with the largest number of total users, possibly because a larger audience is a better target for IFOs and/or spam posting.

The study highlights the need for bot-hunting artificial intelligence (AI), as bots are becoming increasingly complex as technological advancements are made. For example, an in-depth IFO-detection study must utilize more than just comment count and comment speed to identify bots, as clever IFO actors could adjust their bots to post no more or no faster than some pre-determined limit (say, the stream's current mean or median posting speed or count). IFO actors could also use AI to generate comments for their bots, rather than have bots execute comments from a pre-established comment bank. Finally, if an IFO actor develops a bot that posts on a completely random schedule, dynamically generates content analyzed from ongoing streaming audio, visuals, and comments, and actively responds to users, a human analyst will be virtually incapable of identifying the bot. Overall, the complexity of future bots needs to be met with the complexity of AI—AI will be needed to recognize advanced bot algorithms (Manheim and Kaplan 2019).

The authors acknowledge two major limitations with this study. First, it is difficult to determine whether or not a Twitch user is a bot—humans do not possess the ability to distinguish bots from humans except in blatant cases (for example, if a bot posts the same or similar messages at fixed intervals). Second, the criteria may have excluded possible slow-posting bots. Future researchers could develop (or incorporate existing) machine learning and sentiment analysis programs to further refine bot search criteria on Twitch. Additionally, researchers could develop a bot-detection metric or criteria checklist to allow for manual or automated assessment of users, rather than a subjective look over. Finally, researchers should search for countermeasures that actors employ to protect their bots from discovery.

Conclusion

The purpose of this study's was to develop a data-mining prototype, rather than develop a reliable and effective bot-identification program. We did not seek to prove the existence of IFOs on Twitch, but rather show it is possible to identify them if they do exist, and encourage future researchers to use some of our methods to narrow their bot searches. We maintain that our research provides future Twitch IFO- and bot-hunters a better starting point for discovering IFOs and bots.

As the internet audience grows, the potential for IFO development and execution grows. State and non-state actors know the value of IFOs during peacetime and wartime. Twitch is only one vulnerable platform. Online multiplayer games

are additional avenues of influence, as it is relatively easy to create a bot that produces voice or text within games. By introducing IFOs into the platforms used by the average person, IFO actors have the ability to not only change their targets' opinions and behavior, but also alter an entire society's culture (e.g., China's influence efforts in Africa: Kinyondo 2019).

Acknowledgements

The authors would like to thank Petter Kraabøl, who developed the initial tool to download Twitch comments. The authors thank Cecelia Mulvaney and Genevieve Miller for their feedback and recommendations. Finally, the authors would also like to thank Dr. Carter Matherly for providing the opportunity to submit.

Alexander Sferrella holds a BS in Computer Science. His official duties include software development and data analysis, and his interests include following Chinese international politics. He is interested in further research and welcomes opportunities for collaboration.
alexander@sferrella.com

J. Z. Conger holds a BS in Biology and a BA in Psychology, and is graduating with an MS in Applied Psychology in May 2020. His primary research interests include social media, psychological operations, behavioral economics, and improving morale and work environments. He welcomes opportunities for continued research and collaboration.
jzconger@yahoo.com

References

Ahmed, Faraz and Muhammad Abulaish. 2013. "A Generic Statistical Approach For Spam Detection In Online Social Networks." *Computer Communications* 36 (10-11): 1120–29.

Chu, Zi, Steven Gianvecchio, Haining Wang, and Sushil Jajodia. 2010. "Who is Tweeting on Twitter: Human, Bot, or Cyborg?" *ACSAC* 10: 21–30.

Collins, Ben. 2018. "Volunteers Found Iran's Propaganda Effort on Reddit – But their Warnings were Ignored." Last modified August 24, 2018. https://www.nbcnews.com/tech/tech-news/volunteers-found-iran-s-propaganda-effort-reddit-their-warnings-were-n903486.

FireEye Intelligence. 2018. "Threat Research: Suspected Iranian Influence Operation Leverages Network of Inauthentic News Sites & Social Media Targeting Audiences in US, UK, Latin America, Middle East." Last modified August 21, 2018.

https://www.fireeye.com/blog/threat-research/2018/08/suspected-iranian-influence-operation.html.

Howard, Phillip, Samuel Woolley, and Ryan Calo. 2018. "Algorithms, Bots, and Political Communication in the US 2016 Election: The Challenge of Automated Political Communication for Election Law and Administration." *Journal of Information Technology & Politics* 15 (2): 81–93.

Insikt Group. 2019. "Beyond Hybrid War: How China Exploits Social Media to Sway American Opinion." Last modified March 6, 2019. https://www.recordedfuture.com/china-social-media-operations/.

Iqbal, Mansoor. 2019. "Twitch Revenue and Usage Statistics (2019)." Last modified February 27, 2019. https://www.businessofapps.com/data/twitch-statistics/

Kinyondo, Abel. 2019. "Is China Recolonizing Africa? Some Views from Tanzania." *World Affairs* 182 (2): 128–64.

Lee, Kyumin, James Caverlee, and Steve Webb. 2010. "Uncovering Social Spammers: Social Honeypots + Machine Learning." *SIGIR* 10: 435–42.

Loyola-Gonzalez, O., Monroy, R., Rodriguez, J., Lopez-Cuevas, A., & Mata-Sanchez, J. I. (2019). Contrast Pattern-Based Classification for Bot Detection on Twitter. *IEEE Access, 7*, 45800-45817. doi:10.1109/access.2019.2904220

Manheim, Karl and Lyric Kaplan. 2019. "Artificial Intelligence: Risks to Privacy and Democracy." *The Yale Journal of Law and Technology* 21 (106): 106–88.

National Telecommunications and Information Administration. 2018. "Digital National Data Explorer." Last modified June 6, 2018. https://www.ntia.doc.gov/data/digital-nation-data-explorer#sel=homeInternetUser&demo=&pc=prop&disp=chart.

Pew Research Center. 2018. "Social Media Use in 2018." Last modified March 1, 2018. https://www.pewresearch.org/internet/2018/03/01/social-media-use-in-2018/.

———. 2019. "Social Media Fact Sheet." Last modified June 12, 2019. https://www.pewresearch.org/internet/fact-sheet/social-media/.

Prier. "Commanding the Trend: Social Media as Information Warfare." *Strategic Studies Quarterly* 11 (4): 51–85.

RAND. 2009. "Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities." Last modified August 16, 2016. https://www.rand.org/news/press/2016/08/16.html.

RAND. 2016. "US Social Media Strategy Can Weaken ISIS Influence on Twitter." Accessed March 12, 2020. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG654.pdf.

Reddit. 2019. "An Update on the FireEye Report and Reddit." Accessed February 1, 2020. https://www.reddit.com/r/announcements/comments/9bvkqa/an_update_on_the_fireeye_report_and_reddit/.

Roose, Kevin. 2018. "Social Media's Forever War." Last modified December 17, 2018. https://www.nytimes.com/2018/12/17/technology/social-media-russia-interference.html

Sander, Barrie. 2019. "Democracy Under the Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections." *Chinese Journal of International Law* 18 (2): 1–56.

Stanford Internet Observatory. 2019. "Evidence of Russia-Linked Influence Operations in Africa." Last modified October 30, 2019. https://fsi.stanford.edu/news/prigozhin-africa.

Twitter. 2019. "New Disclosures to our Archive of State-Backed Information Operations." Last modified December 20, 2019. https://blog.twitter.com/en_us/topics/company/2019/new-disclosures-to-our-archive-of-state-backed-information-operations.html.

Wang, Alex Hai. 2010. "Detecting Spam Bots in Online Social Networking Sites: A Machine Learning Approach." *Data and Applications Security and Privacy* 24: 335–42.

Yang, K., Varol, O., Davis, C. A., Ferrara, E., Flammini, A., & Menczer, F. (2019). Arming the public with artificial intelligence to counter social bots. *Human Behavior and Emerging Technologies, 1*(1), 48-61. doi:10.1002/hbe2.115

Zakrzewski, Cat. 2019. "The Technology 202: Researchers uncover Russian-style Information Operation ahead of UK Elections." *Washington Post.* Last modified December 3, 2019. https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2019/12/03/the-technology-202-researchers-uncover-russian-style-information-operation-ahead-of-u-k-elections/5de550a788e0fa652bbbdb17/.

A New Russian Realpolitik: Putin's Operationalization of Psychology and Propaganda

Joseph Pagen

Abstract

For two decades, Vladimir Putin has held the highest levels of position and power in Russia. The leader and his collaborating elites harness an enduring Russian identity and methodically design a path for a manipulated society to eagerly regain legitimacy, respect, and relevance. This qualitative and exploratory study examines Putin and his apparatus's efforts to unify Russian society and expand its influence through the cultivation and operationalization of specific psychological theories. Through theory triangulation, thematic coding, and analysis of relevant and current open-source material, convergence demonstrates Putin's disciplined understanding and deliberate management of Russian identity and perception. Evidence indicates Putin's comprehensive and synchronized approach to achieve a spectrum of policy objectives. This study challenges the traditional notion of leadership's rational pursuit of self-interest by showcasing Putin's operationalization of power politics, propaganda efforts, and malleable internal workings of an exclusive society for both manipulation and exploitation.

Keywords: Putin, Russia, image theory, humiliation theory, identity theory, psychological domain, sixth domain

Una nueva Realpolitik rusa: la operacionalización de la psicología y la propaganda de Putin

Resumen

Durante dos décadas, Vladimir Putin ha mantenido los más altos niveles de posición y poder en Rusia. El líder y sus élites colaboradoras aprovechan una identidad rusa duradera y diseñan metódicamente un camino para que una sociedad manipulada recupere su legitimidad, respeto y relevancia con entusiasmo y ganas. Este estudio cualitativo y exploratorio examina los esfuerzos de Putin y

 doi: 10.18278/gsis.5.1.5

su aparato para unificar la sociedad rusa y expandir su influencia a través del cultivo y la operacionalización de teorías psicológicas específicas. Mediante la triangulación teórica, la codificación temática y el análisis de material de código abierto relevante y actual, la convergencia demuestra la comprensión disciplinada de Putin y el manejo deliberado de la identidad y la percepción rusas. La evidencia indica el enfoque integral y sincronizado de Putin para lograr un espectro de objetivos de política. Este estudio desafía la noción tradicional de la búsqueda racional del liderazgo del interés personal al mostrar la operacionalización de Putin de la política de poder, los esfuerzos de propaganda y el funcionamiento interno maleable de una sociedad exclusiva tanto para la manipulación como para la explotación.

Palabras clave: Putin, Rusia, Teoría de la imagen, Teoría de la humillación, Teoría de la identidad, dominio psicológico, sexto dominio

一个新式的俄罗斯现实政治：普京对心理学和（政治）宣传进行操作化

摘要

二十年来，弗拉基米尔•普京一直掌握着俄罗斯的最高地位和权力。这位领导人及其幕僚控制着一个长久的俄罗斯身份，并有条不紊地为一个被操控的社会设计一条道路，以迫切且急需的方式重新获得其合法性、尊重和相关性。本篇定性探究式研究检验了普京及其政府通过对特定心理理论进行发展和操作化，以期统一俄罗斯社会和扩大其影响力所作的努力。通过理论三角测定、主题编码、对相关及当前开源材料进行分析，得出的结果证明普京系统地理解了俄罗斯身份和感知，并有意对其进行管控。证据表明了普京对实现一系列政策目标采取的全面同步方式。本研究通过展示普京为实现操纵和剥削而对一个排外社会的权力政治、政治宣传工作、可调整的内部工作进行操作化，（进而）挑战了关于领导者理性追求自身利益的传统理解。

关键词：普京，俄罗斯，形象理论，羞辱理论，认同理论，心理领域，第六领域

Introduction and Background

Despite efforts of select analysts, policymakers, and academics to force a deliberate iconoclasm and properly jettison the rudimentary assumptions and oversimplified conclusions drawn from conventional thinking and residual Cold War framing, two former superpowers, the United States and Russia, do their part to live up to old expectations. Instead of attempting to go beyond "the orthodoxy of assumed animosity that keeps Russia and the United States from finding negotiated common ground," the two countries remain locked in a dynamic geopolitical chess match involving nuclear weapons, military forces, geographic proxies, and varying ideologies (Crosston 2018). Just like during the Cold War, heightened discourse, diplomatic action, and military posturing from both sides reinforce and amplify power politics and different forms of propaganda. The populations of both nation-states seem not only proud of their ideological entrenchment but also willing and determined to enshrine the amplification of their long-held identity and reinforced convictions.

The crumbling of the Soviet Union and the Berlin Wall brought with it an unfamiliar and uneasy unilateral power structure. The world, as everyone knew it, along with the many neat political theories and institutions, turned on its head. America, perceiving itself as an undisputable superpower, quickly claimed victory at the end of the Cold War, championing both its model republic and spirited liberal institutions. For over a decade, the US confidently showcased to a global audience its accomplishments and effectiveness against its former Soviet foe. Out of the shadows of the Soviet Union, a new modern Russia realized its loss of legitimacy, respect, and relevance. Almost overnight, the vast preponderance of laypeople and analysts perceived the Iron Curtain and all its unifying features to be exposed and erased. Notwithstanding this humiliating descent, the Russian identity and its entrenched political institutions seemed determined to prevent the quick and dramatic transition to some form of liberal democracy and free-market society.

Despite the West's dramatic and impactful victory during the Cold War, Russian society staggered forward with only its perceptions, identities, values, and images. One man, a former Soviet intelligence officer named Vladimir Putin, was able to rise from the ashes to consolidate and capitalize on the tightly held Russian identity. The President of Russia and his cadre of loyal oligarchs undoubtedly hold power and influence Russian society and politics. By skillfully and practically directing the complex Russian political system and exploiting various weaknesses and divisions in the international arena, Putin has been able to unify the once directionless and fragmented Russian society and expand its sphere of influence. He has methodically challenged and chipped away at the West's post-World War II standing throughout the world. This success is not brought about by chance or luck but by a systematic understanding and deliberate management of the unique

Russian identity and perception. It is Putin, who skillfully exploits, manipulates, and reinforces power politics, propaganda, and the malleable psychological internal workings of the collective Russian society.

The purpose of this study is to examine how Putin and his collaborating governmental apparatus has unified Russian society and expanded its sphere of influence by deliberately cultivating and integrating humiliation, identity activation, and image manipulation with more traditional sources of influence. This study argues that Vladimir Putin's and various Russian pro-government apparatuses' current domestic/foreign policy success, including the degradation of Western credibility, is a result of the comprehension, exploitation, and reinforcement of select psychological theories and traditional concepts of propaganda. This research intends to dissect the particular strategy and intentions of the Russian leader over the last two decades. It conducts a pre- and postmortem of operationalization and manipulation efforts relating to the preferred Russian power apparatuses psychological theories of choice.

The conclusions and the data drawn from this research aim to add to the knowledge that serves both international relations and political psychology interests. Scholars and practitioners around the globe currently find themselves in a time period when it is easy to incorrectly surmise that Russian leadership is merely attempting to recreate the Soviet Union (Crosston 2018). It is wrong for theorists to simply dust off rigid and simplistic theories and paradigms. It is essential to examine in detail various constructivist lenses and theories that explain internal factors, motivations, and perceptions that end up having impacts on actions, policies, and attitudes. This research intends to advance the overall conversation about Russia's deliberate manipulation within its growing sphere of influence by combining various psychological theories and reinforcement techniques. This research showcases the comprehensive and synchronized approach that Russian leadership has engineered in an attempt to achieve a spectrum of foreign policy goals and degrade Western power and stability.

Examining an Orchestrated Russian Resurgence

Traditional theories of international relations would lead one to believe that most politics involve the rational pursuit of self-interest. However, "a more accurate picture of human beings as political actors is one that acknowledges that people are driven or motivated to act in accordance with personality characteristics, values, beliefs, and attachment to groups" (Cottam et al. 2010, 1). Individuals are not robots, but rather imperfect information processors who are influenced and manipulated as they try to find stability and purpose in a complex world. To put it in less sophisticated terms, "people are driven to act by internal factors such as personality, attitudes, and self-identity, they evaluate their environment and others through cognitive processes that

produce images of others, and they decide how to act when these forces are combined" (Cottam et al. 2010, 1).

The concept of a dynamic and influential leader who reinforces a society's specific identity and perceptions is not new. However, Putin's ability to skillfully incubate, manipulate, and exploit a unique blend of current and historical perceptions/images, emotions, and an enduring Russian social identity is both impressive and distinctive (Torbakov 2015). For two decades, Putin labored to salvage and reconstitute a "historic Russia," determining that his version of a political system was "the best instrument available to secure the state's integrity" (Torbakov 201, 444). Since taking power, the current President of Russia has embraced varying shades of propaganda and *Realpolitik* as tools of reinforcement and amplification in his efforts to exploit the Russian political system and sphere of influence.

Putin has not only actively taken the reins in his efforts to restore Russian standing and prominence in the world, but has also begun degrading Western influence and cohesion. Tempered by the pragmatic realization that it is not possible to recreate the Soviet State, he deliberately chose to shed the many deficiencies and anchors associated with communism, despite knowing full well there is considerable nostalgia for Russia's linchpin role in the former Soviet space (Hutcheson and Petersson 2016). Putin has been able to deliver social and economic progress to a Russian population eager for tangible results. By utilizing the framework of the political psychology theories of humiliation, social identity, and image, this paper helps readers conceptualize how Putin creates measurable success throughout Russian society.

It is a common misconception that Putin is trying to reconstruct the old Soviet Union (Crosston 2018). A more detailed examination shows that the current President and former Prime Minister of Russia does not intend to resurrect the former Soviet Bloc, but instead exploit and weaponize the characteristics and the mechanisms of order, prosperity, and greatness (Hutcheson and Petersson 2016). Thus his efforts allow the country to thrive while disregarding the elements that let the system flounder. This study assesses the following research questions. How has Vladimir Putin combined, applied, and exploited the political psychology theories of humiliation, identity, and image to consolidate influence and produce achievements in Russian society? Why has the Russian leader embraced propaganda and *Realpolitik* when attempting to pursue political goals? How has Putin capitalized on the malleable internal psychology within his sphere of influence?

Relationships and Key Themes

Drawing on the psychology theories of humiliation, identity, and image, this research examines active Russian policies, goals, motivations, and actions to address the research questions stated above. Despite a US Cold War victory, the new century brought with it a post-Soviet foreign

policy that emphasized Russian "wisdom to understand—ahead of the United States—the important truth that polyarchy is the form of governance that rules the world ... that the conflict in the world politics is the sign of a new era and ... conflict was caused by an overall decline of the influence of the West and opposition to the global rearrangement of power by the United States" (Beak 2009, 459).

With past discourse, Putin declared "to the United States and the West that the U.S.-centered unipolar model in which only 'one master' and 'one sovereign' exist is not only unacceptable but also impossible in today's world, that a new 'architecture of global security' has to be established, and that Russia is not merely a counter-hegemonic state, as it is a leading designer of the new order" (Beak 2009, 458). With a muddled American foreign policy in flux between a Pacific pivot and an enduring Middle East commitment, Russia's leadership and ruling elite remain determined as ever to reshape the outcomes of and the conclusions drawn from the collapse of the Soviet Union.

Putin and his sculpted security apparatus keenly understand the realities of the post- Soviet security psyche. Struggling to compete with the United States and sustain a worldwide power projection image and conventional arsenal, the Russian leadership recognizes the benefits of cultivating and exploiting other types of power, including political, social, and informational ones, in an attempt to bridge the gap between the new Russia and the West. Putin and his governmental apparatus deploy deliberate propaganda against not only foreigners, but also target their efforts against a manipulable domestic mass. Against a Russian psyche, Putin propagates "the idea that Russia is not worse than Western countries, also, to give the impression that Russia is prepared for war" (Rațiu and Munteanu 2018, 193). In this study, "propaganda" encompasses the entire spectrum of possible influence operations, political warfare techniques, active measures, and soft power approaches. For the purposes of this study, the term "propaganda" describes public or covert influence operations that intentionally "aim to affect cognitive, physiological, motivational, ideational, ideological, and moral characteristics of a target audience" (Larson 2009, 3).

This study intends to build on the foundation set by Lebow (2009), *A Cultural Theory of International Relations*. Similar to Lebow's work, this alternative framework of psychological constructivism breaks away from the predictable realist and neoliberal camps and provides ample evidence of combinations of psychological theories that affect the international arena and specific foreign policies. Building on the most "spirit-based world concept," Lebow declares:

> ... international systems were actors are driven not by fear and security dilemma but instead by the desire to bolster pride and self-esteem in their individual and collective identities. In such systems, honor and standing are

> the coin of the realm, and the adult important international pecking order is established through frequent resort to armed conflict. (Hyman 2010, 461)

Putin frames political actions and methods in traditional *Realpolitik* terms. The Russian leader is known for his pragmatic utilization of systems, techniques, and modalities. However, at the same time, he ensures the careful attention and consideration of political, psychological, and constructivist realities to harness and deliberately manipulate target audiences for power consolidation and opposition suppression (Hutcheson and Petersson 2016). Artfully engineering and operationalizing psychologically manipulable variables, Putin has more successfully than not met emergent challenges to his legitimacy and political agenda (Hutcheson and Petersson 2016). Putin's deliberate focus, reinforcement, and weaponization of the three selected theories enable him to become the primary decider and authority of Russia's present and future.

It would seem that Vladimir Putin mastered "the art of ruling ... finding a way to derive benefit from ... the feelings of others and not in wasting one's own energy in order to destroy them. [Putin] is capable of liberating himself from blind control of his own feelings [and] is also capable of exploiting the feelings of others for his own purposes" (Nadskakuła-Kaczmarczyk 2017, 340). The Russian leader understands these theories do not have to be used in isolation; often, the salient principles and elements intertwine, infuse, and complement one another. However, with careful political and psychological assessment and refinement, specific tailoring and formulation can be used to achieve/spread the optimal and desired effects of two of Putin's essential objectives and narratives:

> 1) Russia is rising from its knees and because of that the West, first and foremost the United States, declared war on Moscow in order to preserve its diktat in world affairs. 2) Although threatened on all sides by implacable enemies, Russia has nothing to fear so long as Putin is at the helm, not only will he protect the motherland, but also, he will recover the [Russian] status being viewed and therefore respected again. (Aron 2016)

Putin has made it clear to the international community that he will not be cornered into a specific hardened political ideology. He is determined to avoid making the same mistakes that former Soviet leaders made. Using a variety of realist and constructivist foundations, he is tenacious in remaining adaptive to ever-changing domestic and international political landscapes. He is committed to making modern Russia a respected member of the international community once more. He is resolute in his acknowledgment of the maintenance and the projection of the image required for a specific national identity.

For two decades, Putin has occupied the world stage and has vaulted Russian activities and aspirations back into the mainstream global headlines.

Both Western and Russian media covered the spectrum in detailing Putin's persona and actions during this time period. However, no existing research has proven the causality between combinations of specific psychology theories and present-day Russian political goals and power methods. This research aims to fill the current gap allowing several critical themes and an illustration of the resultant bifurcation to emerge.

The review of varied primary source material highlights Putin's unique manipulation of specific psychological constructivist theories that facilitate and reinforce his overall pragmatic and power politics approach. Through analysis, the following themes emerge. First, since the fall of the Soviet Union and the floundering of the new underdeveloped "westernized" Russian system, the emergent domestic and international political power player, Vladimir Putin, has tapped into the unique Russian identity. He has forcefully constructed specific images and narratives and deliberately forced differentiation among social categories of target audiences to consolidate power, enhance stability, and achieve a variety of *Realpolitik* political goals that are meant to bring Russia the international respect and prominence that the country feels it deserves. Second, despite being calculated and pragmatic in his political approaches, Putin relies heavily on the combined effects of humiliation theory, social theory, and image theory to consolidate his power structure and influence various target audiences in order to project and facilitate heightened social categorization, tailored schemas, and specific political aspirations. Finally, Putin and his Russian political apparatus have embraced and deployed an entire spectrum of propaganda vehicles and techniques used to reinforce the salience of and weaponize these select political psychology theories.

Research Design

Through the application of three psychological theories, Putin assessed the government's efforts to unify Russian society and expand its sphere of influence. In this study, the first step is to evaluate the various political psychology theories that have been operationalized and reinforced by Putin's effective use of propaganda and power politics. The second step is to analyze the goals, intentions, and recent successes of both Russian leadership and society. Through thematic coding and analysis of relevant and current open-source materials, the convergence indicates Putin's disciplined understanding and deliberate management of Russian identity and perception. Qualitative evidence from over two-dozen primary and secondary sources concludes and explains how Putin has harnessed and operationalized the effects of these theories to his advantage.

This research article takes a qualitative and exploratory approach in studying the direct effects of a polarizing yet consolidating Russian influence by the Putin administration to actively target and coax the internal workings of various groups and schemas. Russian leadership and the post-Soviet society's best attempt to achieve desired politi-

cal goals and fulfill societal motivations and ambitions is a holistic and complementary approach. This research highlights and examines exploitable and malleable elements of specific psychological theories and the active measures that reinforce them.

Data points from journalistic interviews, peer-reviewed academic journals, specific subject-matter books, and relevant congressional testimonies were gathered and discovered. The data exhibiting Russian leadership's capitalization and exploitation of specific psychological theories and the application of propaganda and active measures in its efforts to amplify and anchor these political-ideological frameworks were thematically coded. These developed categories were linked through the process of axial and causation coding; inductive and inductive methods formed meaningful relationships.

Successful Post-Soviet Resurrection

The post-Soviet reality left millions dazed, confused, and in search of a new identity. For those who lived under the former Soviet banner, the general consensus was that "the end of the Cold War was Russia's equivalent of the Versailles Treaty ... a source of endless humiliation and misery" (Aron 2016, 1). From the chaff and the political confusion of an early Russian experiment with Western democracy, an unsuspecting ex-Soviet spy emerged, who was immediately tasked by a crippled and directionless Russian society to recover the economic, political, and societal clout was needlessly squandered by a rigid and uncompromising ideology. While the West turned its attention to new strategic priorities in the Middle East, Putin effectively tapped into a historical and societal identity, exposed and exploited intergroup realities, and capitalized off emotions related to the downfall of the Soviet Union. Doing this, Putin carefully and deliberately massaged a security and political apparatus in his image. This refined vehicle of influence and authority was repeatedly employed to amplify and reinforce Putin's distinctive and successful blend of power politics and constructivist realities.

To date, Putin has attained a string of domestic and international successes. He has not only regained a firm and controlling hold on internal information sources and mediums, but has seemingly quelled the chaos and the various insurgent "color revolutions" at the Russian doorstep. The Russian leader has "liberated" entire Russian enclaves in Crimea in Eastern Ukraine, ensuring his portrayal as the true protector of the Russian people. In Chechnya, he personally led a successful anti-terror campaign he deemed equivalent to the perceived noble and required Western crusade against Islamic terrorism. In addition, for many proud Russians, the Putin-directed "humanitarian intervention" in Syria is portrayed as legitimate and necessary due to a perceived lack of any appropriate and moral Western response (Crosston 2018).

Since taking the reigns as Russia's leader, Putin has surprised the West with a reinvigorated patriotic mobilization and consolidation. The inner-workings of which present "an unprecedented challenge: a highly personalistic authoritarianism, which is resurgent, activist, inspired by a mission, prone to risky behavior for both ideological reasons and those of domestic political legitimacy, and armed, at the latest count, with 1,735 strategic nuclear warheads ..." (Aron 2016, 1). For better or for worse, Putin is determined to control Russia's destiny personally. With the unbendable components of authority and nationalism, Putin considers his actions justified and in the interest of Russian society. He believes Russia's "goal is to reinforce our country, to make our country better for life, more attractive ... more valuable, to turn our country into something that could respond swiftly to the challenges of time. To strengthen it from the internal political point of view, and to strengthen our external political stance as well. Those are the goals we are pursuing. [Russia is] not trying to please anyone" (Stone 2017, 205).

Whether a matter of fact or perception, Putin has successfully resurrected Russian legitimacy through a series of domestic and international successes. The transformational Russian leader has forced the West to re-examine and reconsider Russia's relative power and international standing. Moreover, the entire Russian people now feel that they have successfully provided the world with a credible alternative to the dominant and imposing liberal paradigm (Nadskakuła-Kaczmarczyk 2017).

Putin's Propaganda Integration

"Although there are numerous discussions between scholars and military thinkers regarding whether the Russian information warfare is truly 'a new way of war,' a certain aspect of Russian strategy is 'that information now has primacy and operations, while a more conventional military forces are in a supporting role'" (Rațiu and Munteanu 2018, 193). Whatever blend of information operations, active measures, covert spying, political warfare, or soft power initiatives the Russian government sanctioned, it was meant not only to influence policy, but also to deliberately cause division within a consolidated liberal Western culture and security alliance (Chivvis 2017). Putin has ensured a "whole of government" approach by forcibly and deliberately integrating power politics, propaganda methods, and select political psychological theories. Through a variety of mediums and modalities, Russian propaganda once again has tried to invade and cloud the cognitive minds of a variety of target audiences in an attempt to influence desired actions. The new battleground, "from a Russian perspective, is the people's mind, the necessity for hard military power being minimized" (Rațiu and Munteanu 2018, 193). With this paradigm shift, the Russian leadership has chosen to integrate propaganda with calculated power politics in its efforts to create tension, confusion, doubt, and weakness by slowly eroding faith in the institutions and systems that have long served as the pillars of liberal democracy (Chivvis 2017).

Russian propaganda production is not new to the world. However, Putin and his governmental and security apparatus have re-engineered and deliberately tailored the system to be successful in the twenty-first century. Speaking bluntly, General Breedlove, former Supreme Allied Commander of NATO, noted that Russian propaganda "was the most amazing information warfare blitzkrieg we have ever seen" (Gerber and Zavisca 2016, 80). Select messaging, identity reinforcement, and image manipulation by an entire host of sophisticated propaganda methods support Putin's desired end state to have Russian political and social values esteemed higher than the West's. Hostile perceptions of the US "have taken hold in Russia, where nearly 70% of the respondents view [the] United States as an enemy, and an additional 15% see the United States as a rival" (Gerber and Zavisca 2016, 85). Through official statements, mass media, social media, paid agents, and funded nongovernmental organizations, the Russian security apparatus has been able to slowly infect areas that have traditionally been outside Russia's sphere of influence. At the same time, the same systems have turned inward. They have been used to engineer a consolidated narrative, identity, and image against the Russian people who have seemingly willingly abdicated their cognitive defense mindset and stance to a new Russian leader for the promise of stability, direction, and resurgence. There is currently an entire constellation of structured and funded Russian "civil society" institutions and media outlets (Helmus 2018). Hackers, troll farms, *Sputnik News*, and *Russia Today* are the modern Russian equivalents of the T-34 tank; instead of penetrating the physical battlefields, these mediums force cognitive penetration, allowing a manipulated narrative and amplified differentiation within an entire spectrum of target audiences.

Deliberately choosing to make it a priority, the Russian government allocated over $1.4 billion to international and domestic propaganda (Van Herpen 2016, 74). The influence campaigns in the Soviet era and under President Putin represent a "long-term, indirect, and low-risk approach to undermine and weaken an opponent from within in order to promote political objectives and alter the correlation of power in Moscow's favor in order to win the clash of civilizations with the West" (McCauley 2016). Putin and his many controlled networks believe that they can deliberately change attitudes and ideas through the art of persuasion. They understand that they can effectively reinforce existing trends and beliefs to solidify and differentiate the realities of an intergroup process. The current employment and widespread usage of propaganda allow the Russian leader to influence masses near and abroad. This approach causes them to believe that the Russian past "reflects the happy future of present-day Russia .... [The Russian people] don't expect a happy future to come in the form of modernization or the form of approaching the westernized world. [With this], the future lies in the Soviet past of Russia" (Van Herpen 2016, 77).

Putin's Humiliation Capitalization

From Ivan the Terrible, Peter the Great, Lenin, and Stalin, the immense Russian landscape has been governed by a variety of dynamic and powerful figures. Authoritarian and hierarchical in nature, these guided and forced Russian constituencies into subjugation through various revolutions, wars, and ideologies. This collective history of these past leaders contributed to a uniquely developed and entrenched schema and identity among the Russian populace. Both the Russian elite's and laypeople's embrace of a historically bound identity has often associated with the tenets of toughness, resiliency, collectivism, stability, realism, and paternalism.

Alfred Evans highlights a distinctive Russian identity that mutated from its history of specific conditions and traditions. Evans states, "from the very beginning, Russia was created as a super-centralized state. That's particularly laid down in its genetic code, its traditions, and the mentality of its people" (Evans 2008, 903). The Russian people who bore the brunt of horror and destruction during World War II, who saw a cosmonaut ascend to the outer reaches of space before anyone else, who cherished the advanced technology and quantity of their nuclear arsenal, and who bore the many burdens behind the Iron Curtain, all shared a specific and hardened identity fully incorporated into their collective and individual psyche.

Using Saurette's humiliation theory as one of its foundational points, this study begins to identify specific Russian emotional factors of Russian leadership and society relating to how "humiliation ... can act as the basis from which to theorize and investigate its influence in global politics" (Saurette 2006, 496). The variety of emotions and values, including, honor, respect, and mythology, are at the forefront in explaining Putin's motivations and the Russian apparatus's desire to tap into the critical and collective humiliation element widely entrenched in Russian society. Specific Russian dynamics, including humiliation, were experienced for a certain period after the fall of the Soviet Union. This humiliation dynamic has been captured and molded, allowing the Russian government to dictate a specific influential Russian national/foreign policy.

The unforeseen collapse of the Soviet system brought about an unexpected change of the longstanding bipolar international paradigm. Mikhail Gorbachev's and Boris Yeltsin's progressive and reformative *perestroika* platforms encouraged many Russian patriots to hope a new Russia would successfully transition to an economy and political system similar to the West. However, some of Russian society and some Russian elites were more resistant and unaccommodating to the dramatic changes that intended to mimic Western values and conventions. The transformation was haphazard, uncertain, muddled, and embarrassing.

The collective Russian people lost the authoritarian sources of direction and stability to which they had become accustomed. Russian society neither witnessed nor felt the great Western economic downfall that many citizens were expecting. For its part, the West was neither fully open and accommodating in embracing its former foe nor willing to fully incorporate them with the same liberalized respect and values they had now taken for granted. The West projected a collective "fear that the former communist world represented a 'Wild East'; an area populated by violent people who, given half a chance, would love to tear each other apart" (Whitehall Papers 2008, 43). Russian elites and governing bodies were subjugated to being lectured and preached to by their perceived culturally inferior, more recently established countries throughout the West.

> In 1991, Russians lost [their] buffer, the legacy of their greatest generation. With their country falling apart, Russian leaders had no choice but to accept this loss for as long as Russia would remain weak. The 1990s were a terrible decade for Russia, what a great decade for the West. For the Russian leaders and many regular Russians, the dominance of the West came at the expense of Russia's loss in the Cold War. (Senate Rept. 115–40)

Despite being uncertain, vulnerable, and alone, Russian leaders thought that they had collective assurances from NATO decision-makers that the former foe would not exploit the new international realities and power dynamics. However, the Western security institution was quick and aggressive in capitalizing on its perceived final victory against a vanquished Cold War foe. NATO leaders rapidly developed policy and action sets to incorporate new countries that had exited the Soviet's physical and conceptual sphere of influence. Former Warsaw Pact strongholds, such as Poland, Hungary, and the Czech Republic, were quickly integrated and allowed to reap the institutional (security) and cognitive (stabilization) benefits of joining the matured Western defense alliance. NATO's "enlargement apparently broke a promise given to Moscow when the Warsaw Pact dissolved, in undertaking that the West would not seek to benefit from Russia's weakness" (Whitehall Papers 2008, 42).

This deliberate encroachment happened again with the incorporation of countries such as Bulgaria, Romania, and Slovakia, and later, in 2009, Croatia and Albania, into the growing Western defense alliance. However, in 2004, the admittance of countries such as Latvia, Lithuania, and Estonia into the European Union and NATO inflicted a perceived national trauma on the fragile Russian psyche. The "absorption of the Baltic republics into the European Union and NATO have been a bitter pill and, for people continue to think in all fashioned military terms, a strategic dagger pointed at Russia's throat" (Daniels 2007, 8). The West's welcoming of these three countries at the Russian Federation's doorstep, with large populations of ethnic Russians, was

perceived as a deliberate and calculated power grab meant to humiliate and embarrass the former superpower. These three countries had a powerful and enduring historical identification with the "motherland." The Russian people, along with Russia's defense apparatus, could not understand why NATO, whose sole purpose of existence was to defend the West against the Soviet Union, was now even allowed to exist. The newly perceived psychological and cognitive assault and humiliation by an unchecked unilateral institution was a watershed moment for the directionless post-Soviet state.

Persevering Kremlin ideologists and significant factions of former Soviet people soon sensed an embarrassing loss of control and autonomy with the intentional development of in-groups and out-groups (Crosston 2008, 33). This exacerbated humiliation dynamic decreased the strength and self-esteem of the collective Russian identity. With the rest of the international community watching, the humiliator stripped away an entrenched set of prized self-perceptions that were highly valued by a specific people and their leaders in their new infantile state (Saurette 2006, 507). Putin perceived the West, particularly US attitudes and intentions, as omnipotent and consciously flagrant. "[A]fter the end of the Cold War, a single center of domination emerged in the world, and those who found themselves at the top of the pyramid tempted to think they were strong and exceptional, they knew better" (Crosston 2008, 102).

After taking the reins as Russian President in 2000, Putin set a new course for Russia, one in which he was determined not to repeat the rigidness or shortcomings of the former Soviet Union or the perceived degrading, incompetent, and impotent strategies of Yeltsin and Gorbachev. Putin invoked a new political model to counteract the sustained humiliation instigated by the West. His formulated system incorporated unique combinations of loose ideology, firm conservative values, and a rigid political dynamic embedded in paternalism. All of these elements were used to firmly reestablish specific degrees of consciousnesses and internal assumptions that were deemed suppressed not only by Russian society, but also by Putin himself. His triggered counter-humiliation efforts aimed at regaining international respect amid the perceived loss of both image and identity. Putin declared, "Russia is a country with a history that spans more than a thousand years and particularly always use the privilege to carry out an independent foreign policy, we are not going to change this tradition ..." (Daniels 2007, 8).

While serving as either President or Prime Minister over the last two decades, Putin has exploited and operationalized a perceived campaign of humiliation against the Russian people and their diaspora. Instead of attempting to re-engineer a distinctive Russian identity into a particular set of Western culture and norms, Putin embraced and weaponized past humiliations through a variety of propaganda vehicles used to exacerbate and intensify differentiation and emotions, thus expanding the social comparison. This enabled him

and his government apparatus to solidify power, achieve critical international and domestic political objectives, and, when required, to begin to erode the unified Western coalition. With these efforts, "Russia's strategy of influence seeks to alter the perception of—if not halt and eventually reverse—Central and Eastern Europe's Euro-Atlantic enlargement and orientation, which has the added benefits of breaking U.S. and Western dominance of the international and democratic liberal order, restoring Russia's historic sphere of influence, and returning to a bipolar organized world" (Conley et al. 2016).

The Russian masses credited Putin's policies and achievements with their newly restored sense of legitimacy, self-respect, and international importance. To date, the Russian population seems more than willing to endure a new paternalism well above that of Western standards to fill the void of security and collectivism left over from a perceived crusade of humiliation by the US and its Western allies. Many think that Putin exhumed "the type of Russian state that older citizens want, and the citizenry would likely allow anything other than an autocratic state in which citizens are relieved of the responsibility for politics ... and imaginary foreign enemies are invoked to forge an artificial unity" (Charles River Editors 2014).

For over a decade, the former Soviet spy-turned-politician addressed past Russian political blunders that negatively resonated in the developed Russian psyche. By successfully combining constructivist realities and *Realpolitik* actions as a counterbalance against historical humiliators, Putin empowered a Russian population to regain their self-esteem and direction. However, if Putin exposes his nation's possible economic or military weaknesses, like Gorbachev and Yeltsin did, he may be disregarded and cast to the footnotes of Russian history.

Putin's Successful Image Utilization

Utilizing the work of Alexander et al. (2105), this study advances the notion in which "image theorists suggest that the ideas about other actors in the world affairs are organized into group schemas, or images, with well-defined cognitive elements ... comprised of cognitions and beliefs regarding the target nation's motives, leadership, and primary characteristics" (28). The Russian leadership's ability to frame specific perceptions of in-groups and out-groups has allowed it to consolidate power and depict the West as culturally and structurally inferior. The newly reinforced image it portrays to both in-groups and out-groups enables the emergence of a perceived equally credible Russian alternative to the once dominant Western values and institutions.

Putin has determined that an "enemy image" is the primary perception to be exploited, constructed, and advanced. "With enemy image, one considers the other nation (the West) as evil, opportunistic, and motivated

by self-interest. The nation's (Western) leaders are also assumed to be highly capable, but untrustworthy. The enemy image results when an international relationship is characterized by intense competition, comparable compatibility/power, incomparable cultural status" (Alexander et al. 2015, 29). After a series of perceived humiliating actions by NATO and the West and the encompassing embarrassment of the failed experiments of communism and *perestroika*, Putin harnessed this collective and amplified emotion to differentiate his sphere of influence from the West. Through constant exploitation and propaganda reinforcement, Putin's calculatingly framed enemy image is singled out for maturation among the Russian masses. With this operationalization, the West "is perceived as relatively equal in capability and culture. In its most extreme form, the diabolical enemy is seen as irrevocably aggressive in motivation, monolithic in decisional structure, and highly rational in decision-making" (Cottam et al. 2010, 54).

Early on as president, Putin stated to the Russian Federal Assembly that "above all else Russia was, is and will, of course, be a major European power" (Feklyunina 2008, 609). However, due to NATO's encroachment and failure to fully incorporate the new Russia into the Western system, Putin shifted this well-intended perception and imagery, stating, "Russia has always perceived herself as a Eurasian country. We have never forgotten [that] the main part of Russian land is in Asia" (Feklyunina 2008, 609). This manipulation and shifting of imagery allowed the leader to be, at times, centrist in his direction and intentions. This calculated vagueness provides "something for everyone"; it facilitates the motivations and the desires of many business elites who desire to integrate with the established West. At the same time, it cleverly allows Russia to have its own identity. The average citizen is thus entitled to feel proud, unique, and established despite enduring the collective failures of communism, the unfulfilled promise of post-Soviet Union reforms, and the perceived Western onslaught of mental and physical encroachment.

The current Russian government and societal psyche embrace "global affairs as being the exclusive, realist domain of Hobbes and Machiavelli; life is brutish and nasty. In sum, the preservation of power it is not moral or immoral but rather amoral since the pursuit is simply about capability and effective strategy" (Crosston 2008, 103). The Russian military ventures into Chechnya, Syria, Georgia, and Eastern Ukraine prove Putin's appeal through *Realpolitik* actions and frames of reference. Conscientiously framed military actions now ensure that the Russian nation is viewed as not only powerful, but also as invoking its right to self-defense. In Chechnya, Putin has used the same patriotic language and themes to defend the homeland that the West has invoked in its seemingly never-ending "war on terrorism." Putin passionately stated in a personal interview:

> we will destroy those who resort to arms. And we will have to create a local elite, which understands that it is in Chechnya's

> interests to remain part of Russia. As things stand today, any discussion of any status outside the framework of Russia is out of the question .... Only one thing works in such circumstances—to go on the offensive. You must hit first and hit so hard that your opponent will not rise to his feet. (Gevorkyan et al., 2000, 168)

In 2008, Putin's unexpected military intervention in the independent state of Georgia seemingly caught the West off guard. The Russian military's full display and integration of hard and soft power highlighted the new efficacy of Putin's cleverly engineered state. Despite the West's attempts to characterize Russia's actions as illegal and aggressive, invoking a deliberately built enemy image for his domestic audience and diaspora, the Russian president successfully solidified the narrative that he and the Russian military were in fact "protecting the lives and dignity of our citizens, wherever they may be, as an unquestionable priority for our country. Our foreign policy decisions will be based on this need. He will also protect the interests of our business community abroad. It should be clear to all that we will respond to any aggressive acts committed against us" (Crosston 2018, 145).

This narrative was tapped again for the intervention in Crimea and Eastern Ukraine. Putin and his supporting constituents felt justified in their actions to "liberate" and "defend" parts of the historically held "motherland" where millions of ethnic Russians were living. The new narrative is very similar to the age-old one in that the specific identities and cultures of ethnic Russians were not only being suppressed, but were being conspiratorially exploited and eroded by Western interests and manipulations. The Russian leadership determined that the illegitimate, seemingly Western-inspired "color revolutions" needed to be counterbalanced by securing the exceptional Russian identity and image. Putin wanted to be portrayed as a protector of "his" people; whether those people were actually within Russia's physical borders did not matter. The Russian people and defense apparatus wanted to contradict an ever-looming and newly reinforced paranoia and theme, ensuring that the West did not possess unilateral, unchecked power that directly contradicted Russian society's enduring conservative values and paternal preferences. In 2014, Putin solidified his opinion and the "us versus them" theme, stating, "the crisis in Ukraine, which was provoked and masterminded by some of our Western partners in the first place, is now being used to revive NATO. We clearly need to take all of this into consideration in planning and deciding how to guarantee our country's security" (Sochor 2018, 47).

During Syria's current civil war, Putin and his constructed apparatus of influence have advanced a step further. Not only have they defended their interactions with the same tonality and justifications used by the West in its Middle East excursions, but they have also attacked and embarrassed the West for setting the conditions for disaster and failing to take proper actions to

rectify the situation. On the one hand, Putin can speculate, "northern Caucasian fighters participating in the Syrian war will return to their homeland and continue the fight in native Russian soil against Russians. This is one of the primary reasons for military intervention in Syria" (Crosston 2018, 146). Putin's appeal for respect and legitimacy in Syria is displayed in another personal interview:

> we very much fear that Syria will fall apart like Sudan. We very much fear that Syria will follow in the footsteps of Iraq and Afghanistan. This is why we would like the legal authority to remain in power in Syria, so that Russia can cooperate with Syria and with our partners in Europe and the United States to consider possible methods to change Syrian society, to modernize the regime and make it more viable and humane. (Sochor 2018, 59)

On the other hand, the full-spectrum Russian propaganda machine is able to invade the cognitive arenas of select audiences with the message that "the Islamic state is a U.S. project to redraw the political map of the Middle East, or that it is used by Washington to either boost America's supremacy in this part of the world or destabilize Russia's Muslim dominated areas in the northern Caucasus, as well as Russia's sphere of influence in Central Asia" (Crosston 2018, 146). It is with carefully projected and purposely engineered statements such as these that Putin influences and solidifies specific impressions within target audiences. The forced categorization and social comparison relating to enemy imagery further entrench Putin's supporters and distance those against him. With these efforts, he not only grows and isolates his supporting base, but he also consolidates his power and popularity. More importantly, these actions facilitate his desired tectonic shifting toward the return of a more straightforward bipolar international paradigm. These steps are one where the new Russia can compete at the military, political, and cultural echelons that it deems to have deserved. Anchoring this simple yet effective message in a Western television interview, Putin expressed his belief that "the world will be predictable and stable only if it's multi-polar" (Feklyunina 2008, 615).

Eicher, Pratto, and Wilhelm (2012) note that "people perceive members of another group as threatening, they tend to demonize the group, which allows them to justify uncooperative even violent behavior towards this group and thereby maintain a positive self-image. Image Theory further states that images are used to filter information and interpret actions of others thus leading to a reconfirmation of the image" (128). Putin relied on this causation to start rebuilding his country's status and structures. He personally targeted various audiences and groups for either greater inclusion or deliberate isolation, ensuring the hardened pride and loyalty of an active in-group that will fulfill not only Russians but also his motives. At first glance, his methodical military and political decisions can be perceived simply as power politics. However, a

major detailed examination uncovers rather salient constructivist inner workings. Using this unique blend of realism and political psychology, Putin knowingly expanded and solidified an in-group population, further ensuring his popularity and reducing any friction or opposition to his domestic or international agenda.

Through various political power moves and influence operations, Russia's leadership has projected a clear international and domestic image. A variety of actions offer the entire continuum of Russian society a sense of pride and hope for the future. By operationalizing image theory, Putin provides a perception of a model of society and government that challenges the Western unipolar paradigm. However, if Putin's weaponizing of image theory becomes tainted or exposed by Western institutions or the credible internal opposition as a farce or extreme manipulation, the current paternal hold on his subjects may weaken. The failure to highlight the developed "us versus them" byproducts of image theory may allow Putin's in-group to create cracks displaying divisions, thus forcing segments to find positive reinforcement and social mobility from an out-group willing to fill the new void.

Putin's Operationalizing of a Unique Identity and Social Identity

The Russian motivation and desire to elevate their own group's status should be in itself enough for a definite intergroup discrimination against the world's only current superpower. However, Putin's task "is more complicated, being the leader of a nation in profound transition from Soviet communist ideology to a new Russian national identity that attempts to bridge 1000 years of Russian history, spanning eras of the czars to powerful oligarchs" (Stone 2017, 3). Hence, an enhanced differentiation, amplified by deliberate propaganda techniques and influencing methods, is required to accomplish this undertaking.

By operationalizing Stets and Burke's (2000) work, and by allowing the combined theory to address macro- and micro-level social processes, this article emphasizes and forms the necessary relationships to a specific Russian social identity and the particular identity that the current Russian leader depicts. The combined theory employment allows the investigation of groups, roles, depersonalization, self-verification, self-esteem, and self-efficacy in Russian society and its leadership apparatus. The approach also provides both the concept, salience, and critical components needed to link Russian propaganda, active measures, and deliberate political action to the anchoring and amplification of the internal and the external cognitive dynamics within the purposely differentiated groups.

Petersson's (2017) research regarding Putin and legitimacy successfully linked "mythscapes" and the particular Russian identity through the Russian leader's influence methods and emotional allegiance to an unambigu-

ous nationalism. To date, Putin has established himself as a faithful and dedicated guardian of the proud and tested Russian identity he attempts to personify. Putin and his political apparatus, led the struggles against any possibility of a recurring humiliation or future squandering of prestige. The Russian leader's political and propaganda systems ensured the vitality of the long-standing political myth and paranoia of foreign encirclement. Throughout history, Russians have associated closely with "the conspiratorial foe, the valiant leader, in the perseverance of the people [these common characteristics] ... bring forth the supreme qualities of the people, [and] are in line with the characteristics often attributed to a charismatic leader" (Petersson 2017).

Putin's identity fits squarely within the optimal Russian historical and social identity. The population has been yearning for a resolute figure as dedicated as Stalin and Lenin, but with compassion and the promise of something better to come. The Russian president is a "mirror in which everyone, communist or democrat, sees what he wants to see and what he hopes for ... Putin was described as intelligent, competent, physically and psychologically healthy, [as] a man who kept to himself, and who was honest and respected abroad. Supporters drew attention to his toughness … strong-willed and decisive" (McAllister and White 2003, 385). It is these identity traits that Putin has relied on to contentiously engineer himself as a powerful, safe, and proud figurehead.

> Throughout his presidencies, Putin has been highly skilled at capitalizing on a small number of overarching political myths, which have tended to dominate the contemporary Russian mythscape. First, there are Russia's aspirations to be recognized as a great power always and unconditionally. As manifested over the centuries, from Peter the Great to Stalin and up to Putin, this belief seems to function as the basic pillar of Russian national identity. The idea of the country [as] being predestined to be a great power, one that will act and be treated with proper respect, seems to be a dominant political myth upon which Russians' 'weness' largely relies. (Petersson 2017)

With the consolidation and promotion of a specific Russian identity, reinforced throughout the world by various influence mediums and propaganda methods, "Putin was able to reconcile policies and groups that in an earlier era would have been in conflict, notably the working class and the aspirational middle-class" (Sakwa 2008, 882). By deliberately remaining uncommitted to a static ideology, Putin's leadership represents "a distinctive type of neo-authoritarianism stabilization that did not repudiate the democratic principles of the constitutional order in which it existed, but which did not allow the full potential of the democratic order to emerge" (Sakwa 2008, 882). This endorsed and propagated concept of sovereign democracy is a

perfect fit for not only Putin, but also the Russian people who were terrified of, and resistant to, an unguided future. Until Putin, the Russian masses did not see an opportunity for their identity to survive after the West's perceived misrepresentations and encroachments. The Russian president spoke for the people, echoing their sentiment by stating, "they have lied to us many times, made decisions behind our backs, placed us before an accomplished fact. This happened with NATO's expansion to the East, as well as the deployment of military infrastructure [at] our borders" (Khrushcheva 2014, 22).

Similar to Stalinism, Putin's tenure of Russian leadership since 2000 offers the Russian populace access to a cause more significant than the individual, but without the flawed and failed political doctrine and ideology. The Russian identity is now consolidated and redirected by Putin's systems as an effective counterbalance against an overreaching, imperial, and over-sophisticated Western foe. The ever-growing base of support that Putin has constructed feels a sense of strong membership due to the maximized differences between Eastern and Western identities. The in-group favoritism and out-group derogation, along with the highlighted partisanship between two historical foes, have "naturally create[d] a bipolar partisanship where individuals characterize [their loyalties] into 'us' and 'them' and exaggerate perceived differences [to favor] their own group" (Greene 2004, 138). Social identity theory and the harvested identity salience, when properly resourced and operationalized by Putin, bleed over and support his already weaponized elements of both image theory and humiliation theory.

To date, Putin guards the precious Russian identity that sweat and blood has forged over several centuries. However, "despite the fact the Russian leader has consistently enjoyed markedly high approval rates and has benefited from charismatic legitimacy," he must be careful (Petersson 2017, 253). He has used a particular blend of conservatism and paternalism to solidify the operational capabilities of identity theory. If he attempts drastic modernization or dramatic cultural inclusion in his endeavor to jumpstart a stalled economy or hindered societal elevation, he risks alienating large segments of the in-group population that he has systematically cultivated since the start of the new century. His current methods thrive on enhanced and clear-cut differentiation; any variable change resulting in non-conformity to the historical Russian identity could prove disastrous for Putin or his "elected" successor.

Conclusion

Post-Cold War security and defense discussion have often centered on technology, complex alliances, and traditional variables of influence. For the last several decades, neoliberal and realist factions have embraced highs and lows in a bipolar arena. However, it is with a new examination of the constructivist and combined elements mentioned above that now proves other frameworks and factors relevant. Expanded research at the

cross-section of psychological theory and more traditional aspects of power will likely provide evidence, relationships, and generalizations that serve policymakers, defense planners, and politicians around the globe. This entire spectrum of decision-makers must now consider the influences, relationships, and limits uncovered between psychological theories, international relations, and domestic politics. By examining these elements, leaders and decision-makers around the globe can now enable mechanisms to anticipate Putin or other world leaders who attempt to operationalize psychological theories to generate power and advance policy.

Through an investigation of three theories, selective propaganda methods, and deliberate *Realpolitik* techniques, this study examined Putin's distinctive and sophisticated integration of power politics and political psychology theory. The distinctive intertwinement and overlapping nature of the operationalized and weaponized elements mentioned above form the foundations on which Putin has started to resurrect the Russian state. These examined elements of influence are only amplified and entrenched by a modern, advanced, and ever-evolving Russian propaganda organism. These independent elements have a direct effect on the holistic approach that has given Putin's constituency hope, respect, and the possibility of a better future against the hardened and prized backdrop of a storied Russian past.

This study demonstrates that Putin's and his various Russian governmental apparatuses' current policy success, including a degradation of Western credibility, results from the comprehension, exploitation, and reinforcement of the psychological theories of humiliation, identity, and image across Russian society. Above all, this article shows that constructive elements, such as psychological theories, can be operationalized and integrated with conventional influencing elements under unique circumstances and encroach on more realist frameworks security and power generation. At the very least, this study "challenge[s] the traditional notion that people act in politics in a rational pursuit of self-interest" (Cottam et al. 2010, 1). Putin and his accomplice institutions understand that behavior is not necessarily rational, but something to be exploited and reinforced through a variety of tailorable variables.

The various audiences around the world must understand that Putin's success and societal and psychological rearmament neither happened by mere luck nor occurred overnight. Putin does not want the world to underestimate his flexible ideology, hardened values, and nationalistic motivations. He understands that there will be setbacks and that results will not always be instantaneous. This transformational leader will continue to refine the operationalization of these psychological theories, propaganda methods, and *Realpolitik* techniques and, if required, will deviate from any rigid political circumstance. Until critics develop a strategy to effectively combat his exemplary differentiation ability and intergroup molding, the Russian leader will continue to be successful at home and abroad.

Joseph Pagan is currently a doctoral student in the Global Securities cohort with American Military University. He holds a MA in Intelligence Studies and a graduate certificate in Terrorism Studies from the same. In addition, he holds a BS in History from the United States Naval Academy. His primary area of research includes Global Security principals to include political-military studies focusing on the Asian-Pacific theater of operations. Highlights from his research include an updated analysis of Okinawan resistance efforts against ongoing U.S.-Japanese militarism. He welcomes opportunities for continued research and collaboration.
Joseph.pagan1424@gmail.com

References

Alexander, Michele G., Shana Levin, and P. J. Henry. 2015. "Image Theory, Social Identity, and Social Dominance: Structural Characteristics and Individual Motives Underlying International Images." *Political Psychology* 26 (1): 27–45.

Aron, Leon. 2016. "Drivers of Putin's Foreign Policy." *Hampton Roads International Security Quarterly*: 1–4.

Chivvis, Christopher S. 2017. "Hybrid War: Russian Contemporary Political Warfare." *Bulletin of the Atomic Scientists* 73 (5): 316–21.

Conley, Heather, James Mina, Ruslan Stefanov, and Martin Vladimirov. 2016. "The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe." *Center for Strategic and International Studies: A Report of the CSIS Europe Program and the CSD Economics Program*, 1–65.

Cottam, Martha L., Elena Mastors, Thomas Preston, and Beth Dietz-Uhler. 2010. *Introduction to Political Psychology*. 2nd ed. New York: Routledge.

Crosston, Matthew. 2018. *Russia Reconsidered: Putin, Power, and Pragmatism*. Dallas, TX: Brown Books Publishing Group.

Daniels, Robert V. 2007. "Flouting Democratic Norms." *The New Leader* (March/April): 6–8.

Eicher, Véronique, Felicia Pratto, and Peter Wilhelm. 2012. "Value Differentiation Between Enemies and Allies: Value Projection in National Images." *Political Psychology* 34 (1): 127–44.

Evans, Alfred. 2015. "Ideological Change Under Vladimir Putin in the Perspective of Social

Identity Theory." *Demokratizatsiya: The Journal of Post-Soviet Democratization* 24 (4): 401–26.

Evans, Alfred. 2008. "Putin's Legacy and Russia's Identity." *Europe-Asia* 60 (6): 899–912.

Feklyunina, Valentina. 2008. "Battle for Perceptions: Projecting Russia in the West." *Europe-Asia Studies* 60 (4): 605–29.

Gerber, Theodore P. and Jane Zavisca. 2016. "Does Russian Propaganda Work?" *The Washington Quarterly* 39 (2): 79–98.

Greene, Steven. 2004. "Social Identity Theory and Party Identification." *Social Science Quarterly* 85 (1): 137–53

Helmus, Todd, Elizabeth Bodine-Baron, Andrew Radin, Madeleine Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega, and Zev Winkelman. 2018. "Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe." *RAND Corporation*, 1–130.

Hutcheson, Derek S. and Bo Petersson. 2016. "Shortcut to Legitimacy: Popularity in Putin's Russia." *Europe-Asia Studies* 68 (7): 1107–26.

Hymans, Jacques. 2010. "The Arrival of Psychological Constructivism." *International Theory* 2 (3): 461–67.

Khrushcheva, Nina L. 2014. "Inside Vladimir Putin's Mind: Looking Back in Anger." *World Affairs*, 17–24.

Larson, Eric V. 2009. "Foundations of Effective Influence Operations a Framework for Enhancing Army Capabilities." *RAND Corporation*.

Lebow, Richard Ned. 2009. "Introduction." In *A Cultural Theory of International Relations*, 1–42.

Nadskakuła-Kaczmarczyk, Olga. 2017. "Sources of the Legitimacy of Vladimir Putin's Power in Today's Russia." *Politeja* 14 (49): 335–49.

"NATO's Enlargement and Russia's Humiliation." 2008. *Whitehall Papers* 71 (1): 40–68.

Petersson, Bo. 2017. "Putin and the Russian Mythscape: Dilemmas of Charismatic Legitimacy." *Demokratizatsiya: The Journal of Post-Soviet Democratization* 25 (3): 235–54.

Putin, Vladimir. 2000. *First Person: An Astonishingly Frank Self-Portrait by Russia's President*. New York: Public Affairs/Perseus.

Rațiu, Aurelian and Alexandra Munteanu. 2018. "Hybrid Warfare and the Russian Federation Informational Strategy to Influence Civilian Population in Ukraine." *Land Forces Academy Review* 23 (3): 192–200. doi:10.2478/raft-2018-0023.

Saurette, Paul. 2006. "You Dissin Me? Humiliation and Post 9/11 Global Politics." *Review of International Studies* 32 (3): 495.

Sakwa, Richard. 2008. "Putin's Leadership: Character and Consequences." *Europe-Asia Studies* 60 (6): 879–97.

Stone, Oliver. 2017. *The Full Transcripts of the Putin Interviews: Oliver Stone Interviews Vladimir Putin*. New York: Hot Books.

Sochor, Daniel. 2018. *Putin In His Own Words: Russia's President Speaks His Mind on International Relations, Politics, Society, Business and Leadership*. CreateSpace Independent Publishing Platform (November 2, 2016), Middletown, DE.

Stets, Jan and Peter J. Burke. 2000. "Identity Theory and Social Identity Theory." *Social Psychology Quarterly* 63 (3): 224–37.

Torbakov, Igor. 2015. "A Parting of New Ways? The Kremlin Leadership and Russia's New Generation Nationalist Thinkers." *Demokratizatsiya: The Journal of Post Soviet Democratization* 23 (4): 427–57.

US Senate. 2017. "Disinformation: A Primer in Russian Active Measure and Influence Campaigns." Hearing Before the Select Committee on Intelligence, 115th Congr., 1st session. Washington, DC: United States Government Printing Office.

Van Herpen, Marcel. 2016. *Putin's Propaganda Machine: Soft Power and Russian Foreign Policy*. New York: Rowman & Littlefield.

Vladimir Putin: The Controversial Life of Russia's President. 2018. Middletown, DE: Charles River Editors.

White, Stephen and Ian McAllister. 2003. "Putin and His Supporters." *Europe-Asia Studies* 55 (3): 383–99.

What's Thinking Got To Do With It? The Challenge of Evaluating and Testing Critical Thinking in Potential Intelligence Analysts

Margaret S. Marangione

Abstract

This paper examines the need for critical thinking skills in intelligence analysts (IA) in the twenty-first century, with the proliferation of false and misleading information, including the weaponization of information and Big Data. Additionally, it reviews concerns about the critical thinking capabilities of millennial and Gen Z IAs against the performance standards of IC Directives (ICDs) 203 and 610. The debate of how to teach and assess critical thinking skills is also considered. The methodology of evaluating critical thinking tests and the results of a critical thinking test administered to IAs is explored against the backdrop of whether testing is valid when hiring analysts.

Keywords: critical thinking, intelligence analysis, analyst, information operations

¿Qué tiene que ver el pensamiento con eso? El desafío de evaluar y probar el pensamiento crítico en analistas de inteligencia potencial

Resumen

Este documento examina la necesidad de habilidades de pensamiento crítico para los analistas de inteligencia en el siglo XXI con la proliferación de información falsa y engañosa para incluir el armamento de la información y Big Data. Además, revisa la preocupación sobre las capacidades de pensamiento crítico del Analista de Inteligencia Millennial y Gen Z contra los estándares de rendimiento de ICD 203 y 610. También se considera el debate sobre cómo enseñar y evaluar las habilidades de pensamiento crítico. La metodología de evaluación de las pruebas de pensamiento crítico y los resultados de una prueba de pensamiento crítico administrada a los analistas de inteligencia se explora en el contexto de si las pruebas son válidas para la contratación de analistas.

 doi: 10.18278/gsis.5.1.6

Palabras clave: pensamiento crítico, análisis de inteligencia, analista, operaciones de información

思维有什么关系？评价和测试潜在情报分析师的批判性思维一事遭遇的挑战

摘要

鉴于错误信息和误导性信息的扩散，进而对信息和大数据进行武器化，本文检验了21世纪情报分析师所需的批判性思维技能。此外，本文审视了有关千禧一代和Z世代情报分析师在情报界指令203和指令610标准方面的批判性思维能力的关切。还考量了有关如何教授和评价批判性思维技能的辩论。在（批判性思维能力）测试是否适用于分析师招聘这一背景下，探究了有关评价该测试和一项由情报分析师完成的测试结果的方法论。

关键词：批判性思维，情报分析，分析师，信息操作

Introduction

> Many people would rather die than think—in fact, they do.
>
> —Bertrand Russell, Nobel Laureate

> 90 percent of analysts don't know the difference between what they know and what they believe.
>
> —Professor Jan Goldman, Intelligence and Security Studies, The Citadel

Critical thinking is a paramount skill for humans overall, and essential for intelligence analysts (IA) in the twenty-first century, with the proliferation of false, misleading, and ambiguous information. The current information arena is also rife with malicious content spread by news sources, state and non-state actors, and trolls. What is very concerning is state actors, like Russia, who leverage information as a form of psychological warfare. One of the few resources against weaponized information is critical thinking. Critical thinking forces us outside of our own psychology to confront biases, dissonance, and logical fallacies.

Additionally, the twenty-first century global information age is ex-

posing us to more people and ideas and to colossal amounts of open-source resources with more data to sift through, synthesize, and evaluate. While technological advances are being made to data-mine these large datasets, data analytics is reliant on the human capability to decode, evaluate, and make inferences so that priorities can be set and decisions and recommendations can be made. Humans think critically; machines process and sift.

Yet, employers in the intelligence community (IC) have been concerned about the critical thinking capabilities of millennial and Gen Z IAs, which have been compounded by intelligence challenges. The IC has had many issues with both training and framework that began to be voiced in the 1990s by intelligence experts and were followed by a series of intelligence reforms after 9/11. The initial solution was the Intelligence Reform and Terrorism Prevention Act of 2004, which created the Director of National Intelligence (DNI). This act also had the goals of information sharing and created analytic standards, including the IC directives (ICDs) 203 and 610, which forced a critical evaluation of the foundational skills needed for IAs and set a benchmark for performance standards in the IC.

Both directives spell out the hard and soft skills needed for twenty-first century IAs. ICD 203 outlines the core principles, assessment criteria, and deliverables for providing analytic rigor and personal integrity to analytic practice. ICD 610 captures the core competencies needed for GS-15 civilian employees. These groundbreaking directives come at a time when experts and agencies have stated that post-9/11 US analytical capabilities and human and technical procedures need to be repaired and replaced to respond to twenty-first-century threats, including the weaponization of information. Meanwhile, the IC and the education community have been debating how critical thinking and the foundation of social science methodology should be taught in bridging the gap from student or active duty military to government analyst.

While ICDs 610 and 203 provide benchmarks, this leaves employers in the IC struggling to find ways to hire IAs with core competencies that meet these standards and to train their current workforce. Employers have to fill in the gaps in the educational experience that many of their employees received in secondary and academic environments. Additionally, the generalist vs. the specialist debate of how critical thinking skills are learned further dilute a clear and pragmatic approach to addressing the challenge of fostering critical thinking.

One approach for employers is testing a potential employee's critical thinking skill base as part of the hiring process; however, identifying appropriate critical thinking measurements can be daunting and expensive. Also, one option is to address the current employees' lack of skillset with tutorials, but before tutorials can be designed, current employees must be tested for their skill levels.

The methodology of evaluating tests and the administration of a critical thinking test will be examined in this article; one of the striking results found in a critical thinking test administered by this author illustrates the IC's concerns. A critical thinking test professionally designed for defense and military employees was given to a random sampling of twenty junior and senior IAs with disparate levels of experience and education, from high school to Master's degrees, and varying levels of military experience. In the domain of precise knowledge, 56 percent of IAs could not anticipate outcomes or see logical consequences (Marangione 2019). Due to the cost of the test, it was administered to a small sample of IAs, but it may explain why the IC is concerned. While addressing this skill gap is doable, it requires an understanding of twenty-first-century challenges, why this critical thinking skillset is perceived as lacking, what constitutes the critical thinking skillset, and the benefits and drawbacks of critical thinking tests as evaluators of employees.

The Weaponization of Information and Intellectual Awareness

Perhaps now, more than ever, it is imperative to address and foster critical thinking because we are living in a world that challenges the truth on many levels. There has never been such a precedent for the ongoing, systematic efforts to deny the truth and sow seeds of suspicion through the purposeful spreading of disinformation. Additionally, with everyone able to author and publish their truth, conspiracy theories, fake science, and hate have found a market. Manipulative actors use new digital tools to take advantage of humans' inbred preference and craving for answers that reinforce their echo chambers. Alarmingly, a Pew Research Study predicted a future information landscape in which fake information would crowd out reliable information. Some respondents in the Pew study even foresaw a world in which widespread information scams and mass manipulation would cause broad swathes of the public to simply give up on being informed participants in civic life (Anderson 2017). This is especially important when it is well known that deliberate misinformation is being spread by Russia and is powerful enough to begin to weaken the foundations of democracy. As detailed in press accounts and the US Department of Justice's February 2018 indictment of sixteen Russian organizations and persons, scores of full-time employees faked news articles, social media posts, and comments on mainstream websites with the intention of influencing US public opinion. During the run-up to the 2016 US election, Russian social media bots reportedly helped drive mainstream media coverage of false stories and even influenced American stock prices (Golson 2018).

The IC's Perspective

The IC is vested in its IAs' critical thinking skills, even though this skill base has been questioned

and challenged with greater frequency internally in the IC and externally by the President, federal agencies, and academics over the last twenty years, especially as national academic scores have declined. To combat this, on June 21, 2007, the DNI signed and implemented ICD 203, Analytic Standards, regulating and providing baseline competencies for the production and evaluation of intelligence analysis and analytical products, mandating critical thinking standards in the IC. This occurred after the IC was called to task in the *Weapons of Mass Destruction (WMD) Commission Report*. The report stated, "Perhaps most troubling, we found an Intelligence Community in which analysts had a difficult time stating their assumptions upfront, explicitly explaining their logic, and, in the end, identifying unambiguously for policymakers what they do not know. In sum, we found that many of the most basic processes and functions for producing accurate and reliable intelligence are broken and underutilized" (Pigg 2009).

These accusations have continued to haunt the IC. Since his election, President Trump has also questioned their reliability and aptitude, tweeting in April 2019, "They are wrong! Perhaps intelligence should go back to school!" (Trump 2019). This was in response to DNI Dan Coats and other senior intelligence leaders contradicting President Trump's assertions on Iran, North Korea, and ISIS. At a news conference on Abu Bakr al Baghdadi's death in October 2019, President Trump commented, "I've dealt with some people that aren't very intelligent having to do with intel" (Baker 2019). While the President's apprehensions are part of his straightforward style, the IC has reasons to be concerned.

In a study by the National Defense Intelligence College on critical thinking and IAs, David Moore examined repeated intelligence failures, including Pearl Harbor, the Cuban Missile Crises, the invasion of Kuwait, and WMD. He states, "While hindsight is an imperfect mirror for reviewing the past, one conclusion to be drawn from a review of the evidence is that critical thinking could have minimized many of the ensuing crises" (Moore 2007). "For example, the Senate noted in its review of the failure [of WMD] that [rather] than thinking imaginatively and considering seemingly unlikely and unpopular possibilities, the IC, instead found itself wedded to a set of assumptions about Iraq, focusing on intelligence reporting that appeared to confirm those assumptions" (Moore 2007). In his article, Moore also mentions a graduate of the National Security Administration's critical thinking and structured analysis class, who attended an IC seminar on counterintelligence that included representatives from all branches of the IC, including Central Intelligence Agency (CIA) and Federal Bureau of Investigation case officers. During the class, the instructor used a case study for students to use to decide how best to analyze and investigate data to find a mole. Differing opinions surfaced, but a common thread appeared among the case officers: follow your *gut* feeling and collect evidence to support that assumption (Moore 2007). From a critical

thinking perspective, this is alarming; critical thinking is not just about putting information together, finding a pattern, then choosing an answer, it is about reducing bias, considering all options available, and presenting options to a decision-maker. Additionally, critical thinking is about paying attention to what and how conclusions are derived and being able to replicate those conclusions through sound methodologies.

Besides the IC, employers and academia are also concerned about the critical thinking skill level that they see in potential hires, employees, and students. Although critical thinking skills are what employers desire and find most essential, the average employer thinks recent graduates are only "somewhat proficient" in critical thinking skills. This means that, while employers think critical thinking skills are 99.2 percent essential, only 55.8 percent of graduates are proficient (Campbell 2019). Critical thinking specialist Randy Kasten believes that critical thinking "is one skill separating innovators from followers" (Crockett 2012). This is supported by other studies that have found critical thinking is not just about thinking clearly or rationally, but also about thinking independently. According to Lee Crockett, author of *Literacy is Not Enough*, "Critical thinking about something means formulating your own opinions and drawing conclusions. This happens regardless of outside influence. It's about the discipline of analysis and seeing connections between ideas" (Crockett 2012). Student and IAs are both under a steady barrage of information and it important they learn how to evaluate what they see and hear every day. They must be able to identify false ideas and look beyond superficial appearances. These skills are paramount in the age of Big Data and fake news. Yet, this skillset, identified as critical and lacking with employees, can be a challenge to foster in millennials and Gen Zs and may not be developed in secondary and college-level education.

The Generation Gap

There is growing evidence that millennials and Gen Zs may have a gap in critical thinking skills; some researchers see one of the causes of this gap as the information age. The reality for most of these workers has been digital media, online transparency, and the internet (the iPhone was launched in 2007 and Facebook was founded in 2004), which encourage the skimming and scanning of info bites. Along with the proliferation of data, how and what is taught has influenced this skill gap. According to Jan Goldman, Professor of Intelligence Studies at The Citadel, who also has over thirty years working in the IC as an advisor, writer, editor, and IA, "We [educational institutions] are no longer teaching critical thinking. It has gone out the window!" (Goldman 2019). Additionally, the habits that differentiate millennials' and Gen Z's working style are inextricably tied to a desire for quick, accessible answers, rather than a drive to think through problems, which is paramount for critical thinking (Botnick 2017). The choice or inability to evaluate and synthesize

information may put millennials and Gen Zs at the lower end of Bloom's taxonomy. Simply defined, critical or analytic thinking means being able to use the higher end of Bloom's Digital Taxonomy or higher-order thinking skills (HOTS), as illustrated in Figure 1. For readers interested in more research about millennials' and Gen Z's critical thinking skills, I refer them to my articles, *Teaching the Millennial Intelligence Analyst,* published in the Global Security and Intelligence Studies Journal in January 2017, and the December 2016 SIGNAL magazine article *Mind the Millennial Training Gap.*

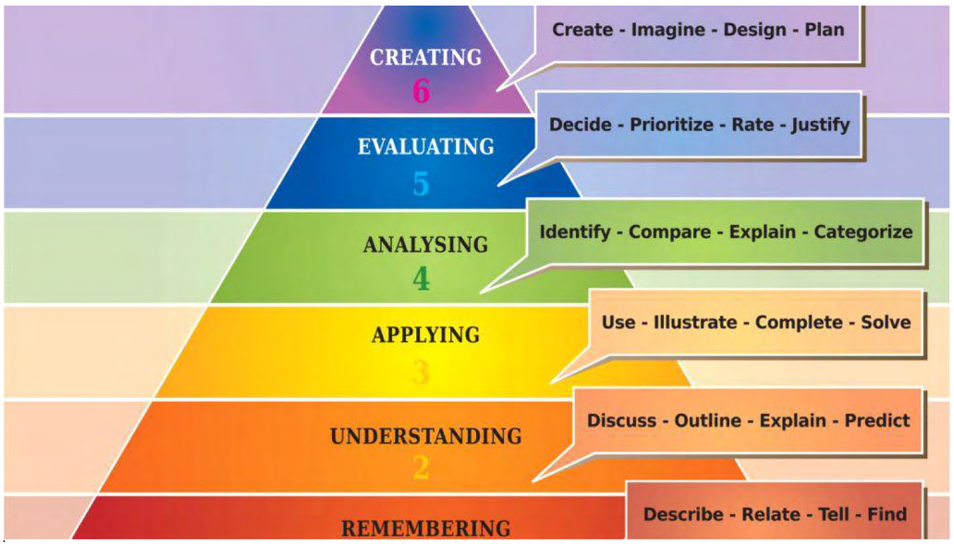


Figure 1: The scaffolding and development of cognition (thinkingmaps.com).

What Is Critical Thinking and Can It Be Taught?

According to Professor William Growley of Georgetown University, critical thinking is "An open-minded but focused inquiry that seeks out relevant evidence to help analyze a question or hypothesis" (Manville 2017). IAs, in particular, have to be able to ask tough questions based on evidence and analysis, to consider and reconsider their cognitive assumptions and biases, and to scaffold what they know from a historic backdrop for forecasting. Additionally, critical thinking goes hand-in-hand with creative thinking and both need to be leveraged for problem solving. For example, one IA explains, "An IA must possess an inquisitive nature. Puzzle solving is another excellent quality found in IAs. Whether you choose crosswords, sudoku, pattern analysis, word search, jigsaw or any type of other puzzles, an IA must grow their mind in order to understand the problem sets that they will work" (Doe 2019.) Professor Jan Goldman concurs. "The best analysts read science fiction" (Goldman 2019).

Cognition can also be developed and enhanced with the structured problem-solving model like solution frequency, which proposes to foster a scaffolded platform for teaching the fundamentals of problem-solving, as shown in Figure 2.

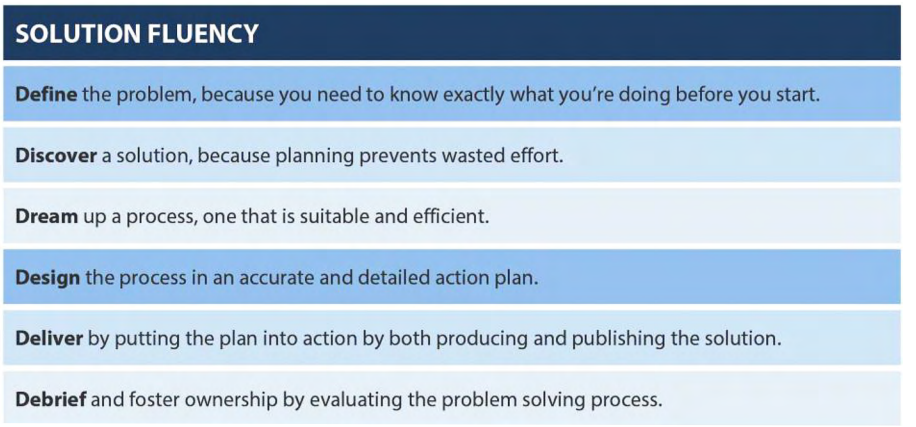


Figure 2: Steps of solution frequency (Marangione 2019).

Along with solution fluency, many propose that there are additional analytical fluencies that students most possess and master. Educating students using traditional literacy standards is no longer enough. If students are to thrive in their academic and twenty-first-century careers, then independent and creative thinking holds the highest currency. This includes solution fluency, information fluency, creativity fluency, collaboration fluency, and analytic fluency. Students must master these fluencies to succeed in a culture of technology-driven automation and abundance and with access to global labor markets. Figure 3 presents an additional production framework of solution fluency for the needs of the twenty-first century.

The Academic Challenge

Ideally, before students become employees, their education should have prepared them to be inquirers, knowledgeable thinkers, and communicators, and to be balanced and reflective—all qualities that encompass critical or analytical thinking. This baseline is often reflected in a college or college department's mission statement and values, which by their very nature, can be a bit vague and obtuse. For example, the James Madison University (JMU) Intelligence Analysis program states, "Students learn innovative ways to structure their thinking to solve complex real-world problems when there is both time pressure and a lack of reliable information. The program highlights the continually evolving nature of intelligence analysis, with an emphasis on employing new academic research into analytic methods" (Intelligence 2019). How students will develop and be assessed in the areas of problem-solving, creative and analytic thinking, collaboration and communication, ethics, action, and accountability are determined

solution fluency	Scientific Method	Writing Process	Media Production	Design Thinking
define	Aim	Prewriting	Preproduction	Define
discover	Background / Introduction	Prewriting	Preproduction	Research
dream	Hypothesis	Prewriting	Preproduction	Ideation
design	Equipment / Method	Draft	Preproduction	Prototype / Choose
deliver (produce)	Experiment	Revision / Editing	Production	Implement
deliver (publish)	Results	Publish	Post Production	Implement
debrief	Conclusion	Review	Review	Learn

Figure 3: Production framework of solution fluency (Crockett 2012).

by each individual professor. Yet, critical thinking is not entirely dependent on the skill base developed in college, but ideally should be developed throughout secondary education. Interestingly, the College Board revamped the SATs, which are taken when students are between sixteen and seventeen years of age, to better assess a high school student's critical thinking (Willingham 2008). In secondary education, due to the reliance on standardized testing (e.g., SATs and the required Standards of Learning (SOL) tests), which hinges on multiple-choice questions, schools do not develop lesson plans around building critical thinking skillsets, but on being able to recall facts, which is a low-level process.

Additionally, it has been proposed that the process of thinking is intertwined with domain knowledge. Anything experienced is automatically interpreted from what a student (or employee) already knows about similar subjects. Familiarity with a problem's deep structure and the knowledge that one should look for a deep structure is inherent in critical thinkers. When a student or employee is very familiar with a problem's deep structure, knowledge about how to solve it transfers well. That familiarity can come from long-term, repeated experience with one problem, or from various manifestations of one type of problem (i.e., many problems that have different surface structures, but the same deep structure). After repeated exposure to either or both, the student or analyst simply perceives the deep structure as part of the problem description. However, it takes a good deal of practice with a problem type before a person knows it well enough to immediately recognize its deep structure (Willingham 2007).

Many classes at the university level adopt meta-cognitive critical thinking paradigms to coursework where a problem's deeper structure is explored. For example, critical thinking can be embedded into scaffolded as-

signments that build on students' skills, knowledge acquisition, and synthesis of information, usually assessed through written research papers, lab reports, and mathematical problem sets. Inherent within writing a research paper are various levels of reasoning that, according to Bloom's taxonomy, promotes higher-order thinking skills and more critical thought in the form of synthesis-level thinking and builds on the prior skill levels in a hierarchical fashion (Wallmann and Hoover 2012). Professor Wallman of Western Kentucky University states, "Arguably, an important component of critical thinking skills is the ability to critically examine and understand published research ... requiring students to critique published research is one way of addressing the goal of teaching students to critically evaluate ..." (Wallmann and Hoover 2012). Research papers inherently require students to evaluate, process, sift, and synthesize information into a conclusion. At their very essence, research papers are problem-based learning activities that sharpen critical thinking skills. However, some college classes utilize multiple-choice tests. It should be noted that multiple choice tests do have their place in assessment as they can be graded objectively without bias and allow for inclusion of a broad range of topics on a single exam, thereby testing the breadth of a student's knowledge. Yet, they should be used with other measurements, and questions have to be developed that allow students to think rather than simply recall facts.

Strides have been made by the American Association of Colleges and Universities (ACCU) to develop guidelines and rubrics for college-level assignments to measure areas in critical thinking, but these guidelines and rubrics are not required mandates for college professors. For example, in the paper *California Teacher Preparation for Instruction In Critical Thinking Instruction*, the authors found 89 percent of college faculty claimed critical thinking as a primary objective of instruction, yet only 19 percent could define the term and only 9 percent were using it in teaching methods on a daily basis (Paul 2007). Interestingly, in *Critical Thinking and Intelligence Analysis,* David Moore (2007) states, "In informal conversations with recent hires at NSA ... fewer than half of these individuals have been exposed to critical thinking skills in college."

The study that has become most emblematic of higher education's failure to teach critical-thinking skills to college students is Richard Arum and Josipa Roksa's *Academically Adrift.* The researchers found that college students make little gain in critical-thinking skills, as measured by students' scores on the Collegiate Learning Assessment (Arum and Roksa 2011). Therefore, it is not surprising that the math skills of college-bound graduates in the United States have slid to their lowest point in fourteen years. For example, an indicator that students were ready to succeed in first-year college algebra fell to its lowest level since 2004, a decline of 46 percent. English proficiency or readiness also dropped to 60 percent for test-takers, from 64 percent in 2015—the lowest level since testing began. In

reading, 46 percent of students were ready to move to the next level of learning, while in science, the metric stood at 36 percent (Crises at the Core 2005).

These scores are supported by many in the teaching field and by literacy experts. Professor Goldman (2019) states, "We don't teach students how to think. The average student has not improved their reading skills since the fifth grade and that is the skill set they come to college with." This is echoed in the seminal book, *How To Read a Book,* by Mortimer Adler, who defines elementary, inspectional, analytical, and synoptical levels of reading. Many argue students' post-high school reading is at the elementary and inspectional level of reading, when at the college level, synoptical reading is expected and assumed to be mastered by college-level students. Syntopical reading requires an individual to perform deep structure analysis by reading and/or analyzing numerous sources, analyzing those sources in relation to one another and to a subject around which they all revolve. Then the individual draws conclusions from the evaluation and analysis—the baseline job description for any IA (Adler, 1972)

In addition to synoptical reading levels, many in the intelligence field feel that being able to communicate orally and in writing goes hand-in-hand with critical thinking and is of equal importance. Defense Contractor and IA Mark Sanders (2019) states,

> The ability to speak and present information well goes beyond writing. An IA must be able to distill huge amounts of data coherently and be able to discern what is critical. For example, I have briefed Chairman JCS [Joint Chief Secretary], Deputy Secretary of Defense, the National Security Council, Under Secretaries, and Ambassadors and every time I had much less time than originally scheduled. In addition to briefing people quickly, I have had to craft one-page decision papers [from larger papers] distilling very detailed technical information to senior leaders – this is an art. The analyst needs to not only impart the knowledge but if interacting with a senior, needs to ensure that what is required, a decision, a policy, an action, is apparent to that individual. I've seen lengthy briefings end badly when I had to ask, "So what do you want me to do?"
>
> The analyst needs to be able to cope with stressful situations, large data sets, conflicting information and maintain focus.

Complementing Mark Sanders is IA and Technical Reports Editor Mark Ashley (2019), who states, "While critical thinking is of utmost importance, it is right next to writing and production. The IC suffers greatly from a *drastic* shortage of strong writers. It is an epidemic. I have seen firsthand how careless articulation and misplaced punctuation can disrupt an entire intelligence message."

The Generalist and Specifists Debate

Further complicating critical thinking is how to develop this skill base; contemporary arguments in critical thinking swing between two camps: generalists and specifists. A key question in the debate is whether thinking skills can exist independently from discipline-specific content in a meaningful way so that the transfer of critical thinking skills is possible. On one side are the generalists who believe "critical thinking can be distilled down to a finite set of constitutive skills, ones that can be learned in a systematic way and have applicability across all academic disciplines" (Willingham 2007).

On the opposing side are specifists who argue that "critical thinking ... is always contextual and intimately tied to the particular subject matter with which one is concerned" (Willingham 2007). The generalist position is the philosophical basis for the standalone, generic thinking skills course, in which students supposedly learn skills that transfer across subjects and domains. But Daniel Willingham (2007) points out that such courses "primarily improve students" thinking with the sort of problems they practiced in the program, "not with other types of problems." This suggests that it is extremely difficult, if not impossible, to separate thinking skills from the content. In other words, critical thinking is only possible after one acquires a significant amount of domain-specific knowledge, and even then, it is no guarantee.

Instead of a debate between these two camps, what might be seen as the best of both worlds is the infusion approach, which suggests that the generalist and specifist approaches can be married, as seen in Figure 4. The generalist perspective provides for a foundation in reasoning and the specifist perspective applies this sound reasoning to specific content.

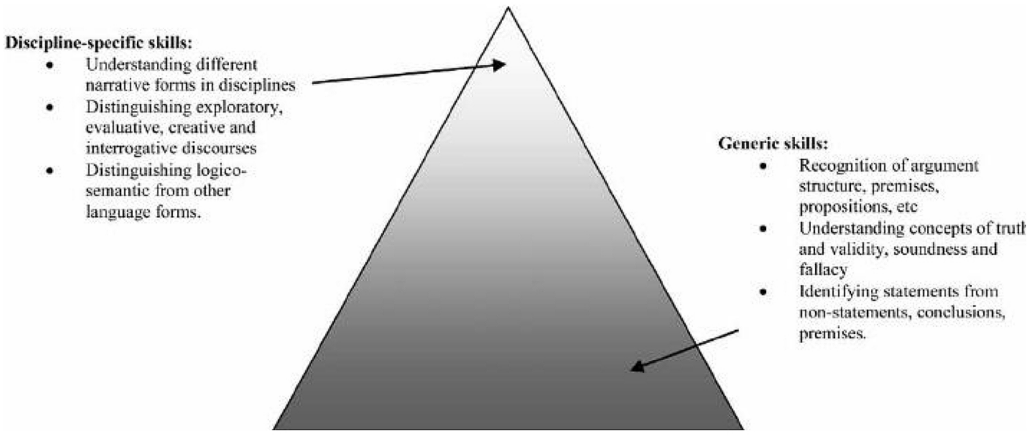


Figure 4. Combining generalist and specifist perspectives (Davis 2013).

Teaching Critical Thinking and the Skill Gap

The challenge then becomes how can critical thinking be taught effectively? In the article, *Critical Thinking; Why is it So Hard To Teach?,* the author points out that critical thinking is not even a skill. Willingham (2007) states, "... teaching [people] to think critically probably lies in a small part in showing them new ways of thinking and enabling them to deploy the right type of thinking at the right time." The author also states that there are metacognitive strategies that once learned can make critical thinking more likely and that domain knowledge and practice are paramount to aptitude, which is supported by the infusion approach of the generalist and specifist perspectives.

Students who take classes in intelligence analysis or complete programs of study, degrees, or certificates in this area are exposed to analytical methodologies and generalist frameworks for structured problem solving and improving critical thinking skillsets. These metacognition strategies, or thinking about thinking, assist students in developing a critical thinking skillset that enables understanding and control of the cognitive processes like not settling on the first conclusion, avoiding biases, ignoring countervailing evidence, overconfidence, etc. Additionally, most intelligence analysis classes teach and stress methodologies, but there are strengths and weaknesses to utilizing methodologies.

Methodology has an advantage because it can be replicated; this is important especially in viewing the IC as a profession that relies on a scientific model. Historically, in the IC, e.g., the Office of Strategic Service (OAS) in 1947, academics performing intelligence analysis were trained in and familiar with rigorous critical thinking. In the 1960s, the employment pool opened up in the IC and with this change, there had to be a codification of thinking. According to Jan Goldman, methodology did not get introduced until Sherman Kent, commonly known as the father of intelligence analysis, along with Richard Heur's analysis of competing hypotheses for observed data. "He [Kent] codified analytic methodologies because IAs' thinking had to be replicated and professional" (Goldman 2019).

In addition to replication, appositive to utilizing methodologies, an analyst has to be able to differentiate and sometimes utilize numerous methodologies. One analyst stated, "I do not limit myself to one methodology but use: competing hypothesis, qualitative, quantitative, mixed-method, what-if scenarios, scenario trees, weighted ranking, probability trees, pros cons and fixes, casual flow and diagraming. Different problem sets require different analytics or a mix of methodologies" (Doe 2019). Mark Sanders (2019) states, "I really like red team approaches where an analyst can think contrarian views. What I look for in an analyst is someone who does not mirror image a viewpoint." On the other hand, some feel that methodologies are dangerous if that is all that is relied upon. Using

methodologies might not correlate to critical thinking because theory has to relate to practice and different methodologies might provide divergent answers to the same problem set.

Complicating the issue is that many new hires in intelligence analysis do not come into the community with a four-year university intelligence degree or exposure to metacognition strategies or analytical methodologies. In a survey of thirty-two new hires for IA positions at a defense contractor, undergraduate degree programs were predominantly in criminal justice, cybersecurity, history, and homeland security. Other degrees included international relations, political science, government, and politics (Wynn 2019). Additionally, many of the IA positions do not require a Bachelor's degree, though it can count towards experience in qualifying for a position level (junior, mid-level, or senior). For a senior position, most positions require specialized training like intelligence courses and ten-plus years' experience. An undergraduate degree could count for up to four years of required experience. Most defense contractors will substitute two years' experience for a Bachelor's degree, and another two years for a Master's degree (Wynn 2019).

Many intelligence positions are staffed by former military analysts who may have a variety of military experience. They may not have taken the Department of Defense military intelligence training classes, and many of those classes might not include analytic methodologies. While the Defense Intelligence Agency (DIA) offers a variety of training venues and training partnerships with other government agencies like the Joint Military Attaché School, Joint Military Intelligence Training Center programs and the National Intelligence University, there might be a variance in how critical thinking is defined, measured, or assessed from instructor to instructor.

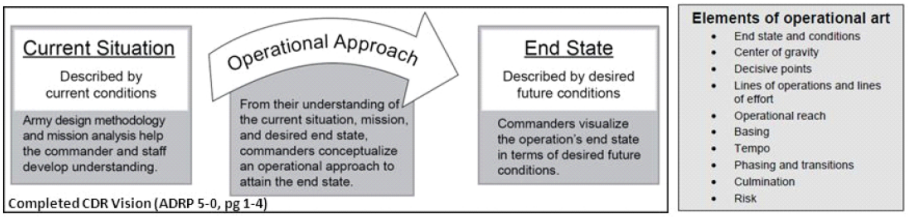
Furthermore, military operational and strategic methodologies, which are dependent on branch and job position, have different targeted outcomes and may require different tools and critical thinking skillsets, as shown in Figures 5 and 6. This disparate approach to how critical thinking is taught, assimilated, and applied does not entail that students in military analysis or employees possess a variety of degrees or education levels lacking in critical thinking skills, but it does point to the challenge for employers to determine the level of critical thinking a new employee from any academic background brings to the job.

Testing IAs for Critical Thinking: A Silver Bullet?

How can employers specifically evaluate the critical thinking skills of potential IAs with such far-ranging backgrounds? One tool in the hiring toolbox may be testing for it. According to the *Harvard Business Review*, there is already a precedent in the industry. "Recent research shows that about 76% of organizations with more than 100 employees rely on assessment tools such as aptitude and personality tests for external hiring. That figure is

Operational Approach

- **Current Definition:** Operational Approach – (DOD) A description of broad actions that the force must take to transform current conditions into those desired at end state. See ADRP 3-0 and ADRP 5-0. (ADRP 1-02, pg 1-27)



- Through operational art, commanders translate their operational approach into a concept of operations and ultimately into tactical tasks. (ADRP 3-0, pg 4-1)
- In applying operational art, commanders and their staffs use a set of intellectual tools to help them communicate a common vision of the operational environment as well as visualizing and describing the operational approach. Collectively, this set of tools is known as the elements of operational art. These tools help commanders understand, visualize, and describe combinations of combat power and help them formulate their intent and guidance. (ADRP 5-0, pg 2-4)

Figure 5: Operational Approach

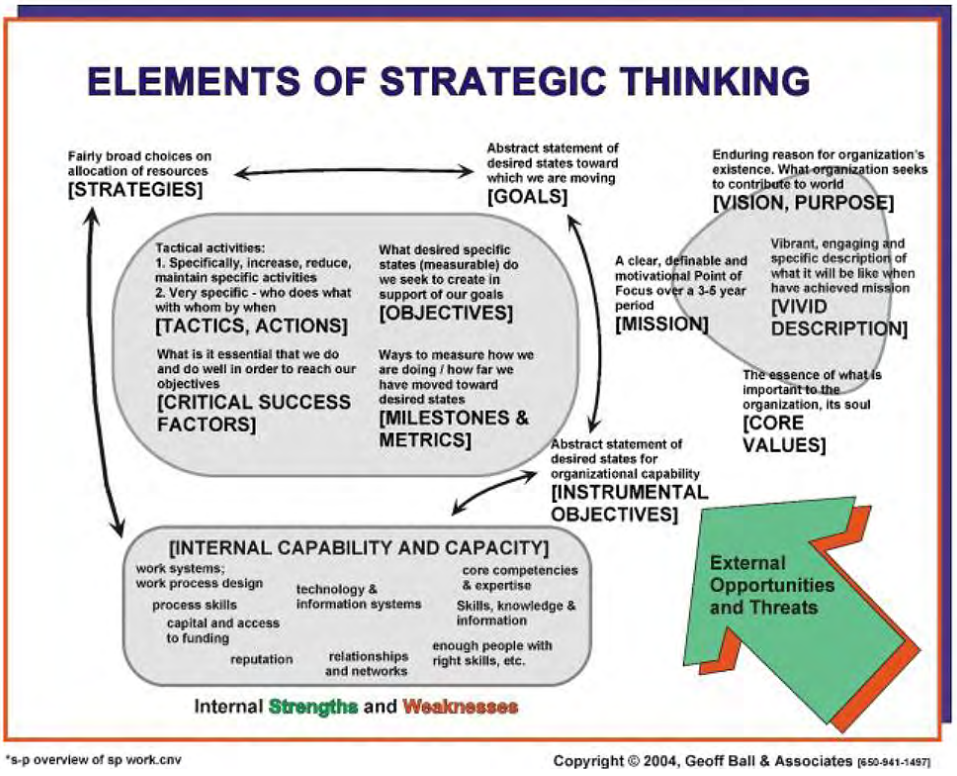


Figure 6: Strategic approach (Geoff Ball and Associates 2004).

expected to climb to 88% over the next few years" (Chamorro-Premuzic 2015). There are numerous online critical thinking tests available from no cost to over $75.00 per test that claim to provide critical thinking assessment. Additionally, some companies provide profile reports that compile the results into specific categories of recognizing assumptions, evaluating arguments, and drawing conclusions. Most tests purport to determine a person's ability to reason through an argument logically and make an objective decision. Some tests claim to measure a person's ability to assess a situation, recognize assumptions, create a hypothesis, and evaluate arguments. Additionally, some tests assert to be able to test a person's ability to distinguish between strong and weak arguments. For example, if an argument is strong it must be directly related to the question and if it is weak it confuses correlation with causation. Deduction questions have test-takers draw conclusions based on the information given in a case study. Interpretive questions ask test-takers to regard the information presented and determine if a conclusion is true and logically follows the information presented. Inferences can also be measured to determine how well a test-taker can draw conclusions from the observed facts.

Evaluating available critical thinking tests, determining if the tests actually measure critical thinking and then deciding if the tests encapsulate the IA skillset is a formative task. Three reviewers, which included this author, an educator, and a college Coordinator of Assessment and Transfer Degrees, reviewed ICDs 610 and 210, studied critical thinking definitions, investigated academic assessments of how critical thinking is taught at the secondary and college level, and finalized a spreadsheet with a list of eleven possible tests out of twenty tests reviewed that seemed to best measure critical thinking skills in concordance with IDCs 610 and 203. Reviewers then evaluated those tests based on cost and content. Using these criteria, reviewers determined that three tests were the best options for final evaluation.

From mid-February through mid-March 2019, three critical thinking tests were taken by the author, the educator, and the coordinator of assessment; each reviewer evaluated the strengths and weaknesses of the test based on the goals of ICDs 610 and 203 for IA competencies. See Appendix A for a detailed review of these three tests' strengths and weaknesses (Marangione and Long 2019).

All evaluators agreed that the tests provide a measurement of competency on a basic level. They measure if a person is low, moderate, or high in applying critical thinking for analysis and decision-making. Subscale interpretations test whether a person can read between the lines, and explore and measure the awareness of some cognitive biases. Additionally, test results provided whether a person can assimilate and evaluate information into conclusions, take into account alternate points of view, and evaluate arguments based on the strength of evidence. Figure 7 provides an illustration of the reviewer's final assessment.

CRITICAL THINKING TEST ASSESSMENTS

TEST A Time Frame: 30-60 minutes. Cost: $28.00 per person & $37 per profile development (20 tests = $1,300).	**TEST B** Cost: E-testing System Orientation - $190.00; 20 Defense Skills at $75.00 each = $1,690.00	**TEST C** Time Frame: 20-45 minutes. Test System Hardware: $116.88, Test System Software: $532.91, Postage/Packing: $146.10 = $795.89
Measures ability to draw conclusions. Reflective component allows participants to provide assessment and feedback.	Two-part test measures critical thinking and personality traits corresponding to participants' critical thinking ability.	Tests critical thinking in an easy to understand way. Judgments applied to everyday scenarios.
Purports to measure confirmation biases and emotional thinking.	The two tests give a solid overview of skills and ability.	Purports to measure critical thinking skills involved when confronted with a general scenario.
Test questions generic to critical thinking; no defense scenarios.	Test questions are specific with many defense/military scenarios that use critiquing and justifying decisions in scenarios.	Test questions generic to critical thinking; no scenarios specific to defense.
Provides a general overview of the candidate: moderate, strong, or weak critical thinking skills.	Provides overall numerical score for critical thinking and a descriptive interpretation.	Provides an overall numerical score of critical thinking.
Provides subscale interpretation for recognizing assumptions, evaluation of arguments, and drawing conclusions in a non-numerical, detail-rich report.	Provides subscale interpretation for ambiguous contexts, precise contexts, problem analysis, quantitative contexts, and evaluation of alternatives with a detail-rich report.	Does not provide subscale interpretation of verbal reasoning, argument analysis, skills in thinking as hypothesis testing, using likelihood and uncertainty, decision-making, and problem solving.
Medium length test with non-military scenarios.	Test is longer in duration with in-depth scenarios; second part evaluates how the tester approaches different scenarios.	Short test length with non-military scenarios.

Figure 7: Critical thinking test assessments (Marangione 2019).

The DIA also administered Test A to a sample of its employees. The concerns that the DIA had regarding the test was how effective the test was in measuring metacognition—thinking about thinking—or measuring whether a potential analyst is capable and aware of the processes used to plan, monitor, and assess one's understanding (Moore 2007). Test A and B, as determined by

the evaluators, did not measure metacognition. Test C had questions that required test-takers to consider their biases, assumptions, and evaluations, but in multiple-choice test format, which was the format for all three tests. The drawback of multiple-choice is that they do not provide qualitative data. Even so, it was determined that Test B was the most effective in measuring critical thinking and included real-world scenarios that applied directly to defense professionals.

Critical Thinking Test B Findings

Test B was administered to a random sampling of twenty junior and senior IAs employed by a defense contractor and working at numerous military locations. Interestingly, in this cohort, individuals who had training in analytic methodologies had low scores on the critical thinking test. In fact, only three IAs out of twenty stated that they used analytical methodologies on the job. Out of those three, one had low scores and two had moderate scores (Marangione and Long 2019). Also concerning is the testing results measuring precise contexts; 53 percent of the cohort of IAs did not manifest this skill, as illustrated in Figure 8.

Because of the cost factor, the test was only administered to a small sample. It is understandable that conclusions cannot be drawn from such small a sample; however, the results appear to support the conclusions drawn by the IC. It should be cautioned that critical thinking skill tests might not predict job-related performance and this is an area for further study. Critical thinking tests are a tool, but only one tool in the toolbox for measuring an employee's critical thinking aptitude or at least their skill level when hired. Some researchers have also postulated that general intelligence ability, as measured by critical thinking tests, does not predict an individual's critical analytic thinking skills. Instead, it found that "critical thinking predicts task performance above and beyond the ability of general intelligence" (Eslon 2018). Also, according to Statistics and Research Methods Professor Hilary Campbell, assessment tests are inherently and seriously flawed, and their results cannot be evaluated in a silo. For example, she feels that assessment tests may just measure a person's ability to take tests (Campbell 2019). Critical thinking tests suggest the importance of measuring and testing critical thinking skills when making evidence-based decisions while hiring, but they are not the only means and certainly should not be used exclusively. Their results suggest the potential benefits of measuring critical thinking skills in the hiring process and testing before and after analytical training to gauge the effectiveness of training.

The Way Forward

Significant research shows that metacognition can be a skill that is developed over time and must be fostered by employers by encouraging and welcoming strategies to employ critical thinking in the workplace. This

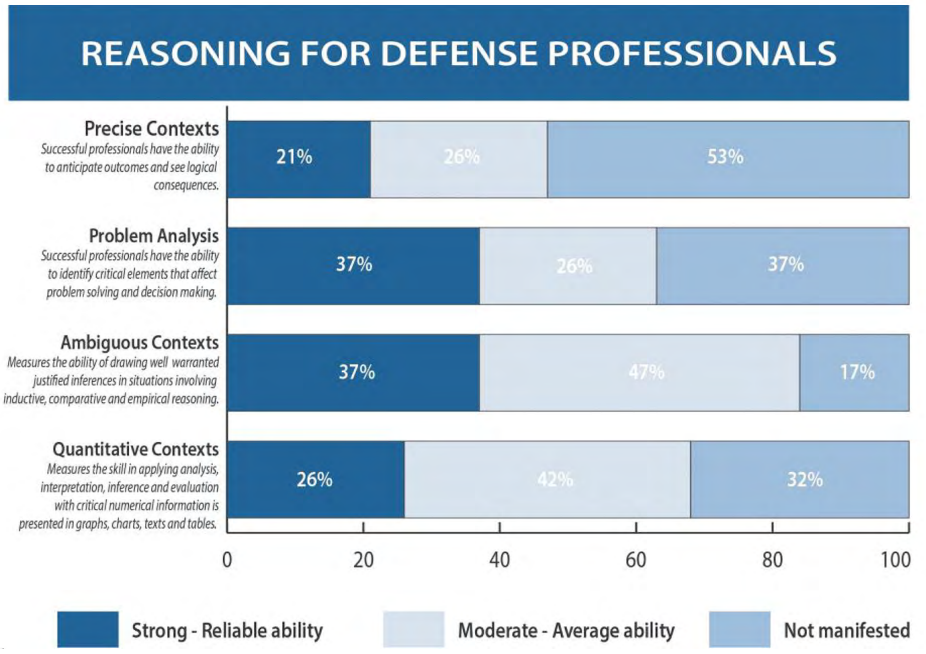


Figure 8: Reasoning for defense professionals (Marangione 2019).

FOSTERING THE METACOGNITION SKILL SET

Provide a workplace environment that supports creative thinking. *Have an environment that encourages and supports out of the box thinking-new ideas and innovations.*

Analysts must challenge and question their assumptions, decisions and evaluations; they also must be pressed to be skeptical and critique a coworker's perspectives. *This fosters self-awareness and metacognition.*

Onboarding process must immediately stress a culture of analysts using creative and critical techniques as a shared problem-solving tool.

Leadership must model these behaviors.

Provide incentives for completing skill-building classes.

Workplace layout that encourages collaboration. *Steve Jobs laid out the bathrooms in Pixar so that engineers and artists would bump into each other (Donfro 2015).*

Build a long-term talent pipeline by partnering with schools through apprenticeships, internships, and continuing education programs.

Figure 9: Fostering the metacognition skill set (Marangione 2019).

SITUATIONAL INTERVIEW QUESTIONS:
Provide a scenario: How would employee break it down or analyze it with evaluation tools? *The focus should be on their thinking process.*
Describe a problem to the candidate with information that is missing. What information should be sought before making a decision? *Ideally, each new question brings a new set of questions and considerations.*
Have the candidate describe a problem they faced in a previous job. *Awareness should be on candidate's rationale and cognitive process.*
Ask candidate to explain if and when they ever questioned the status quo, implemented new policies and procedures, and evaluated their own or a co-workers' cognitive biases.

Figure 10: Situational interview questions (Marangione 2019).

can be fostered through Socratic communication in the workplace and may be best developed in a workplace environment that supports and rewards effective and seasoned analysts, values and encourages continued training, and promotes mentorships and interactions with senior and junior IAs. This is further clarified in Figure 9.

There are numerous steps that an employer can take in assessing new hires; resumes and previous job performance are indicators of skill base and training. Along with critical thinking tests, employers can use situational interview questions to tease out a potential employer's critical thinking skillset, as characterized in Figure 10.

When an employee is on the job, the workplace environment is critical to building the metacognition skillset that many researchers argue is developed through context, mentorship, longevity, and practice. Additional training can be useful for employees; however, as one Chief Executive Officer of a defense company stated, "Buy-in [from employees] can be a challenge. Many analysts feel it is another thing to do in their already busy days. They resent it and do not value the training" (Anonymous 2019). This can be remedied by an onboarding process that clearly spells out the company's training goals, rewards professional development, and offers incentives for programs of studies, classes, and completing tutorials.

For employers, their worries are not just a modern dilemma. Pre-hire assessments have been around at least since the Han dynasty in the third century. Chinese imperial leaders used them to gauge knowledge, intellect, and moral integrity when selecting civil servants. Modern personality and intelligence tests were introduced in the United States and Europe during World War I to aid in military selection. After World War II, companies started adopting them to screen applicants. Today, employers like assessments because they greatly reduce the time and cost of recruiting and hiring. Tests also aid in preventing interviewers from accepting or rejecting candidates based on conscious or unconscious biases. Because

tests can be given remotely and scored electronically, they can widen the pool of candidates. Most importantly, valid tests can help companies' measure three critical elements of success on the job: competence, work ethic, and emotional intelligence. Although employers still look for evidence of those qualities in résumés, reference checks, and interviews, they need a fuller picture to make smart hires.

Partnering and encouraging academic institutions to trail-blaze new measures for fostering critical thinking in the twenty-first century age of Big Data, fake news, and the weaponization of information is also paramount. The University of Washington is at the forefront of making a systematic and organized effort to strengthen critical thinking skillsets at their university, disseminating lesson plans and educational material for free on their website. Their Office of the Provost states, "... it is crucial that we educate our students on how to think critically, access and analyze data, and, above all, question the answers. If our students are going to become leaders, scientists, public officials, writers, businesspeople, teachers—even informed voters—they need these skills .... But now, the need is more important than ever as our devices flash yet another outrageous headline every day" (Baldasty 2018).

The CIA concurs and calls for all twenty-first century citizens to be exposed to tradecraft structured analytical techniques, which can help individuals challenge the mental models which humans can use to sift through abundant information and be aware of the fallacies that humans are prey to. "Schools and academia should consider ways such rigorous [Intelligence] analysis could be brought into curriculums. Ideally, just like every student learns the scientific method in STEM classes, every civics student should learn intelligence analysis techniques" (Golson 2018). The CIA further suggest that there should be an online initiative or a "Master Class taught by former IAs with the goal to encourage Americans to be 'self-conscious about their reasoning process.'" As critical thinking trailblazer, CIA analyst and educator Richards Heuer writes, "[Individuals] should think about how they make judgments and reach conclusions, not just [think] about the judgments and conclusions themselves" (Golson 2018).

Along with the weaponization of information, what has been called the Fourth Industrial Revolution is changing and shaping the students, employees, and the IAs of tomorrow. Many forecasters have predicted that talent and ability will represent a critical factor in the workforce. Talent assessment, recruitment, and employee training and engagement will have to be revisited because an employer will need to find talented IAs whose skills stack up against the high-paced needs of the IC. Complex problem solving, all aspects of critical thinking, creativity judgment, decision-making, and the ability to be cognitively flexible will be paramount. The twenty-first century is taking us to the threshold of a more dynamic and sophisticated digital information age, where technology's impact extends

across domains—cultural, social, business, politics, economics, engineering, medicine, and the IC. It has also taken us to a dangerous threshold, where fake news and the weaponization of information has a growing foothold. Critical thinking will be the foundation of a human's ability to thrive and survive. For employers in the IC, being able to evaluate a potential employee's cognitive ability will be acute, because the IC's most valuable asset is still its analysts, whose skills and values, it can be argued, might be far greater than any other work of technology and relevant fields combined. The security and defense of the United States, the decisions of policymakers, and our relationship with other countries are all dependent on their assessments and evaluations. An IA's skill base must be excellent, critical thinking must continue to be addressed, and some type of baseline testing of potential IAs may be needed. At the very least, testing opens the door for dialogue of skill base and the ways to improve and address critical thinking.

Margaret S. Marangione is a senior researcher for defense contractor, Syntelligent Analytic Solutions. She started her career as an Intelligent Analyst for the CIA and worked as a Security Analyst for Grumman-Northrop. She is a former researcher for the Humanitarian Mine Action Center working directly with the State Department, Department of Defense, United Nations and the Geneva Center. She is the founding editor of the *Journal of Mine Action* and her intelligence–related articles have appeared in the *International Journal of Intelligence and Counterintelligence*, the *Global Intelligence Studies Journal* and *Signal Magazine*. The funding for this article was supported by Syntelligent Analytic Solutions. The author can be reached at Margaret.marangione@syntelligent.com

References

ACT. 2005. "Crises at the Core: Preparing Students for College and Work." http://www.csun.edu/~rinstitute/Content/policy/Crisis%20at%20the%20Core.pdf.

Adler, Mortimer. 1972. *How To Read A Book*. Edited by Charles Van Doren. New York: Simon and Schuster.

Anderson, Janna, and Leann Raine. 2017. "The Future of Truth and Misinformation Online." Pew Research Center Information and Technology. Retrieved from https://www.pewresearch.org/internet/2017/10/19/the-future-of-truth-and-misinformation-online/

Anonymous. 2019. Interviewed by Margaret Marangione. Luray, VA. May 14, 2019.

Arum, Richard and Josipa Roksa. 2010. "Academically Adrift." doi:10.7208/chicago/9780226028576.001.0001.

Ashley, Mark. 2019. Interviewed by Margaret Marangione. Luray, Virginia June 28, 2019.

Baldasty, Jerry. 2018. "Fake News and Misinformation: Why Teaching Critical Thinking Is Crucial for Democracy." University of Washington. Provost's Office, April 23, 2018.

Campbell, Marissa. 2019. *Top Five Skills Employers Look For*. Wichita, KS: Newman University. https://newmanu.edu/top-5-skills-employers-look-for.

Chamorro-Premuzic, Tomas. 2015. "Ace The Assessment." *Harvard Business Review* July. https://hbr.org/2015/07/ace-the-assessment.

Crockett, Lee, Ian Jukes, and Andrew Churches. 2012. *Literacy Is Not Enough: 21st-Century Fluencies for the Digital Age*. Moorabbin, Australia: Hawker Brownlow Education.

Doe, John (anonymous). 2019. Interviewed by Margaret Marangione, Luray, VA. June 18, 2019.

Donald Trump. Twitter Post. January 30, 2019. 9:50 am. Retrieved from https://twitter.com/realdonaldtrump

Goldman, Jan. 2019. Interviewed by Margaret Marangione, Luray, VA. June 12, 2019.

Golson, Preston and Mathew Ferraro. 2018. "To Resist Disinformation, Learn to Think Like an Intelligence Analyst." Central Intelligence Agency Center For Intelligence Studies. March 2018.

James Madison University. 2019. "Intelligence Analysis Major." April 13, 2019. https://www.jmu.edu/academics/undergraduate/majors/IntelligenceAnalysis.html.

Long, Janet. 2019. "Critical Thinking Tests." Syntelligent Analytic Solutions. Internal Report. February 2019.

Manville, Brook. 2017. "How To Hire And Develop Critical Thinkers." *Forbes*. April 26, 2017. https://www.forbes.com/sites/brookmanville/2017/04/23/how-to-hire-and-develop-critical-thinkers/.

Moore, David T. 2007. "Critical Thinking and Intelligence Analysis." *PsycEXTRA Dataset*. doi:10.1037/e509522010-001.

Pigg, Vonn. 2009. "Common Analytic Standards: Intelligence Community Directive # 203 and U.S. Marine Corps Intelligence." *Small Wars Journal*, 1–10. https://smallwarsjournal.com/blog/journal/docs-temp/260-pigg.pdf.

Sanders, Mark. 2019. Interviewed by Margaret Marangione, Luray, VA. June 22, 2019.

SHMR. 2019. "Screening By Means of Pre-employment Testing." September 2019. https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/screeningbymeansofpreemploymenttesting.aspx.

Small Wars Journal. n.d. "IC Directive # 203 and USMC Intelligence." Accessed April 17, 2019. https://smallwarsjournal.com/jrnl/art/ic-directive-203-and-usmc-intelligence.

University of West Florida. 2018. "The Importance of Critical Thinking For Students." https://getonline.uwf.edu/articles/education/critical-thinking-for-students.aspx.

Wallmann, Harvey and David Hoover. 2012. "Research and Critical Thinking: An Important Link for Exercise Science Students Transitioning to Physical Therapy." *International Journal of Exercise Science* 5 (April): 93–96. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4738974/.

Williams, Katie Bo. 2019. "Trump Renews Attacks on US Intelligence Community for Contradicting Him." Defense One. January 30, 2019. https://www.defenseone.com/politics/2019/01/trump-renews-attacks-intelligence-community-contradicting-him/154539/.

Willingham, Daniel T. 2008. "Critical Thinking: Why Is It So Hard to Teach?" *Arts Education Policy Review* 109 (4): 21–32. doi:10.3200/aepr.109.4.21-32.

Wynn, Julian. 2019. "Survey of New Hires." Email interview by author. February 2, 2019. Program Manager, Syntelligent Analytic Solutions

Appendix: Critical Thinking Test Assessments

Test A: Taken February 2019

This test measures the ability to recognize arguments, including assumptions. It purports to measure confirmation biases and emotional thinking. It also measures the ability to draw conclusions. Time frame: 30 minutes.

Strengths:

- Test questions had simple scenarios
- Cost $28.00 per person & $37 per profile development (20 tests = $1,300)
- Easy to follow instructions
- Detail-rich report that included:
    - Evaluation based on norm group: candidate is measured against candidates in their level (managers are measured against managers)
    - Provides a general overview of the candidate: moderate, strong, or weak skill base overall
    - Provides subscale interpretation for recognizing assumptions, evaluating arguments and drawing conclusions (about 3-4 lines of quantitative results)
    - Provides a number of answers that the candidate got correct
    - Gives a percentile for each subscale (skill area) to see where the employee needs further training
- For an additional charge of $37.00, company provides more qualitative data assessment, an appraisal of where the candidate can develop skills in target areas, and a reflective component that allows the candidate to provide their own assessment and feedback
- Quick score results
- Test time: 30-45 minutes, depending on the test-taker

Weaknesses:

- Test questions were sometimes poorly worded.
- Test scenarios vague and general

- Does not measure cognitive biases
- Took **numerous** phone calls and emails to coordinate with a representative for the company—even for simple questions. I would not categorize them as being proactive at all.
- The DIA feels that this test "confuses measuring skills with abilities." Skill: the ability to apply knowledge to specific and practical situations and ability, which is inherent. Skills, ability, and knowledge all must be interwoven in a good IA.
- The scenarios seemed to be generic and juvenile
- There are only three subscales: recognize assumptions, evaluate arguments, and draw conclusions.

Test B: Taken February 2019

This is a two-part test that measures critical thinking and personality traits that correspond to critical thinking ability. Time frame: 30 minutes

Strengths:

- The two tests give a solid overview of both skills AND ability
- Test questions were specific, contained many military scenarios, and were well worded
- Variety of testing questions include numerical scenarios and reasoning
- Representative is proactive, eager to help and eager to learn; companies need to better choose appropriate testing cohort
- Specific tests based on company profile; i.e., defense professionals
- One test measures critical thinking in ambiguous contexts, precise contexts, problem analysis, quantitative contexts, and evaluating alternatives
- Attempts to assess both skills and abilities
- Ability to mix and match from two different genres, i.e. defense and science and engineering mindset.
- Offers six skill areas: ambiguous contexts, precise contexts, problem analysis, contexts, evaluation alternative, and overall

- Detailed analysis of strengths and weaknesses in each skill area
- Approximate test time: 1-1/2 hours depending on the test-taker

Weaknesses:

- Cost is higher than other tests: E-testing System Orientation - $190.00; 20 SE Prof Mindset & Defense Skills at $75.00 each = $1,690.00
- Does not provide any suggestions for follow-up to improve skills
- Does not provide any space for candidate
- Self-reflection
- Does not test for cognitive biases

Test C: Taken March 2019

This is a 20-question test that uses scenarios and asks you to pick assumptions, facts, conclusions or validity scale answers.

Strengths:

- Easy to understand scenarios-simple and straightforward
- Quick (20-minute time frame)
- Test System Hardware - $116.88, Test System Software - $532.91, - $146.10 = $795.89

Weaknesses

- Cost in Euros—price fluctuates
- Scenario questions are repetitive
- Questions do not seem to allow for higher-order thinking
- Too basic to be comprehensive
- Repetitive
- Interview questions to be completed by Syntelligent through an interview with the employee. We must decide what we want to hear; they provide examples of questions.

- Takes up to two days to receive the scores
- Does not provide an actual score for each of the areas: verbal reasoning, analysis, skills in thinking as hypothesis testing, using and uncertainty, and decision-making and problem-solving skills

Recommendations: This is the best market value critical thinking test currently available to test a potential job candidate's critical thinking ability base, but it is flawed and weak in assessment.

Reflecting History: The Basis for Assessing the Future

James Burch

Abstract

The US Intelligence Community has grown immeasurably in the past several decades as it faces the challenges of a growing and diverse global threat environment. Additionally, in a digital age of technology and interconnectedness, intelligence often takes a techno-centric approach, where intelligence analysts focus on key technological issues, capabilities, and programs related to the threat environment. While these issues are of significant concern, it is easy to overlook some of the "soft" requirements that contribute to the understanding of the intelligence problem—namely, a well-grounded appreciation and understanding of history and how it informs a broader understanding of culture and group and individual psychology. Understanding the historical narrative informs an appreciation of the environment, culture, and underlying psychology. Even with its limitations, history provides the intelligence professional with the basis of assessing the future.

Keywords: analysis fundamentals, intelligence analysis, history, information operations

Reflejando la historia: la base para evaluar el futuro

Resumen

La Comunidad de Inteligencia de EE. UU. Ha crecido enormemente en las últimas décadas al enfrentar los desafíos de un entorno de amenazas global creciente y diverso. Además, en una era digital de tecnología e interconexión, la conducta de la inteligencia a menudo adopta un enfoque tecnocéntrico donde los analistas de inteligencia se centran en cuestiones tecnológicas clave, capacidades y programas que se relacionan con el entorno de amenaza. Si bien estos temas son motivo de gran preocupación, es fácil pasar por alto algunos de los requisitos "blandos" que contribuyen a la comprensión del problema de inteligencia, a saber, una apreciación y comprensión

 doi: 10.18278/gsis.5.1.7

bien fundamentadas de la historia y cómo informa una comprensión más amplia de la cultura y psicología grupal e individual. La comprensión de la narrativa histórica informa una apreciación del entorno, la cultura y la psicología subyacente. Incluso con sus limitaciones, la historia proporciona al profesional de inteligencia la base para evaluar el futuro.

Palabras clave: fundamentos de análisis, análisis de inteligencia, historia, operaciones de información

反思历史：评价未来的基础

摘要

面对一个不断发展且多样化的全球威胁环境所发起的挑战，美国情报界在过去几十年里以无法估量的方式扩大。此外，在充满技术与互联互通的数字时代，情报行动时常以技术为中心的方式进行，情报分析师从中聚焦于与威胁环境相关的关键技术问题、能力和计划。尽管这些问题是显著关切，但却容易忽视一些促进理解情报问题的“软”要求，即对历史进行充分评价和理解，以及这种评价和理解如何促成有关文化、群体和个人心理的更广泛的理解。对历史叙事加以理解则能评价环境、文化及背后的心理。即使历史存在限制，它也能为情报专家提供评价未来的基础。

关键词：分析基础，情报分析，历史，信息操作

Introduction

The absence of romance in my history will, I fear, detract somewhat from its interest, but if it is judged worthy by those inquirers who desire an exact knowledge of the past as an aid to the understanding of the future, which in the course of human things must resemble if it does not reflect it, I shall be content.

—Thucydides, History of the Peloponnesian War

The US Intelligence Community has grown immeasurably in the past several decades as it faces the challenges of a growing and diverse global threat environment. Additionally, in a digital age of technology and interconnectedness, intelligence often takes a techno-centric approach, where intelligence analysts focus on key technological issues, capabilities, and programs related to the threat environment. While these issues are of significant concern, it is easy to overlook some of the "soft" requirements that contribute to the understanding of the intelligence problem—namely, a well-grounded appreciation and understanding of history and how it informs a broader understanding of culture and group and individual psychology.

The strategic intelligence professional requires a grounding in history in order to evaluate present and future circumstances. While a deep understanding of history is not a panacea for intelligence analysis, having a well-rounded grasp of history allows for a deeper understanding of the key events, cultural components, and psychological determinants that frame the intelligence issue. In terms of conducting intelligence analysis, it is important to understand that the mission of intelligence is multi-faceted in its purpose and seeks to support several objectives and stakeholders. This article poses the argument that the knowledge of history is essential in evaluating the diverse nature of a threat by providing intelligence professionals with the necessary skills of critical thinking, cultural awareness, psychology, and the understanding of the context of issues.

Background

While an exhaustive background on the topic is beyond the scope of this article, gaining knowledge of history and a fundamental understanding of the issues related to intelligence activities has long been established as a key premise. Sherman Kent, the "father of intelligence analysis" was himself a trained historian. Kent highlights the importance of understanding history as a means of identifying patterns and trends from the past in order to evaluate how actors will conduct policy in the future. Additionally, he highlights the importance of demystifying the past in order to maintain an objective assessment of the future.[1] One can see the echoes of Thucydides in his perspective. Allen Dulles, a key figure in the Office of Strategic Services (OSS) during the Second World War and the legendary Director of Central Intelligence (DCI) during the early days of the US intelligence community highlights the importance of recruiting personnel from academia with "a well-trained mind free of prejudice and immune to snap judgment" to support intelligence analysis.[2] Gaining more than a superficial understanding

1 Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton, NJ: Princeton University Press, 1966), 58.

2 Allen W. Dulles, *The Craft of Intelligence* (Guilford, CT: Lyons Press, 2016), 173.

of history has clearly been highlighted as a key aspect of intelligence analysis.

Dulles further highlights the importance of analyzing historical cases as a fundamental approach to establishing the context of the issues.[3] The literature on analyzing intelligence issues is replete with evaluating cases. Wohlstetter's early analysis of the surprise attack on Pearl Harbor in her seminal work, *Pearl Harbor: Warning and Decision*, delves into the misinterpretation of indicators and strategic warning analysis of a key historical event from an intelligence perspective. Allison and Zelikow highlight the importance of utilizing various analytical models framed in a contextual understanding of the issues to differentiate intelligence analysis in their study of the Cuban Missile Crisis.[4] Lastly, Grabo's foundational work in developing warning analysis specifically highlights the foundational importance of understanding history when developing indicator lists.[5] A knowledge of history is fundamental to placing an intelligence problem within its present context.

As mentioned earlier, an understanding of history is not a panacea for intelligence analysis. In other words, history has its limitations as well. Neustadt and May's work in *Thinking in Time* highlights some of the challenges with using historical analogies to support decision-making. Additionally, May's insight into *"Lessons" From the Past: The Use and Misuse of History in American Foreign Policy* identifies the misapplication of history based on a superficial knowledge or impressions from the past. More recently, there is the challenge with revising or reinterpreting the past based on political perspective. Betts' seminal examination of politicization in *Enemies of Intelligence* and Christian's work in *Channeling the Past* explore this disturbing trend.

Discussion

It is necessary to integrate a historical perspective into a theoretical intelligence framework in order to appropriately frame the need to understand the history behind it. For instance, an example from a military perspective provides tactical-level intelligence that directly supports the warfighter's ability to accomplish both near- and mid-term battlefield and theater-wide conflict objectives. Conversely, strategic intelligence supports national policy objectives that ensure decision-makers are fully apprised on issues within a collaborative framework dealing within an uncertain global environment. These intelligence functions are offensive in nature as they seek to attain strategic advantage in tactical level goals and objectives. Irrespective of the level and differences in time horizons between tactical versus strategic issues, a grounding

3 Ibid., 175.

4 Graham Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis* (New York: Longman, 1999), 2–12.

5 Cynthia M. Grabo, *Anticipating Surprise: Analysis for Strategic Warning* (New York: University Press of America, 2004), 26.

in history provides the intelligence professional with the foundational tools to aid them in discerning the issues while evaluating the context of the conflict in question within its cultural and psychological dynamics.

Intelligence is also a defense-oriented field in which intelligence professionals, agencies, and other stakeholders exist to provide warnings for their assigned customers. In other words, providing a policymaker with sufficient warning of the next surprise attack by an adversary is one of the key functions of the US intelligence community. This core function harkens back to the establishment of the modern-day intelligence apparatus, when President Harry Truman stated:

> A long-felt need for the coordination, on the highest level, of intelligence opinion relating to broad aspects of national policy and national security was probably the principal moving factor in bringing about the creation of the Central Intelligence Agency. The lack of any provision for the prompt production of coordinated national intelligence of this kind was one of the most significant causes of the Pearl Harbor intelligence failure.[6]

Within the context of strategic warning, the grounding of history is an essential component in trying to assess and forecast threats. Understanding historical context, cultural, psychological nuances, and past cases serve as the basis to evaluating potential threats to US and Allied interests. For example, evaluating the case of the Yom Kippur War (1973) highlights Israelis' flawed assessment within this context. Misapplying history as a result of Israel's victory in the Six-Day War (1967), underappreciating Egypt's capacity for employing deceptive tactics within the framework of Islamic culture, and the psychology overestimating Israel's strategy, military prowess, and intelligence capabilities to provide an early warning were significant contributors to Egypt's initial success in the war.[7] The need for focused strategic warning analysis and an appreciation for the regional historical, cultural, and psychological context within the nature of intelligence issues is paramount.

The genesis of the US intelligence community was also framed with a theoretical perspective regarding the need to both coordinate and collaborate, while supporting strategic to tactical objectives that also provide a strategic warning mechanism in its infrastructure. Within this framework, there was an inherent need to coordinate intelligence issues at the highest level ***with*** the policymaker, in order to pursue national security objectives. The critical nature of the relationship between the

6 US Government, Intelligence Survey Group, *The Central Intelligence Agency and the National Organization for Intelligence: A Report to the National Security Council* (Washington, DC: Government Printing Office, 1949), 5.

7 Uri Bar-Joseph, *The Watchmen Fell Asleep: The Surprise of Yom Kippur and Its Sources* (Albany, NY: The State University of New York Press, 2005), 25–33.

intelligence professional and the policymaker has been at the forefront of concern since the inception of the community.[8] Maintaining analytic objectivity and protecting intelligence activities from politicization were but a few of these concerns. Much of the US wartime intelligence experience at the strategic level was influenced by the British model, which was highly evolved and sophisticated in its intelligence support to policy generation and implementation. Second, there was also a clear necessity to develop an entity that would be fully capable of warning policymakers in advance of any major potential threats toward US interests. After all, the surprise attack at Pearl Harbor (1941) still loomed in the minds of policymakers and intelligence professionals as they streamlined the creation of the US intelligence community that came out of the National Security Act (1947). As a result, the tragedy of Pearl Harbor directly influenced the establishment of the first-ever US peacetime intelligence community—something that had previously been viewed as being antithetical to US democratic norms.

Despite the clear purpose and motivation to establish the US intelligence community, the actualization of this two-fold construct has been problematic. The simple adoption of community structures modeled along British lines does not mean that the problems and issues with synchronization would disappear—particularly if they do not account for unique US cultural issues. This is one of Professor Zegart's arguments: the separation of powers, majority rule, frequent elections, and political compromise inherently diminish the capacity of the US intelligence community to provide objective assessment amid a fractious political and policymaking process.[9] Intelligence is not the only vote at the policy table. A well-reasoned intelligence assessment based on a sound historical, cultural, and psychological understanding of an issue may not necessarily take the day. After all, the grounding of history may serve as a foundational premise for the assessment and may lead to a greater appreciation of the underlying cultural and psychological issues; however, intelligence professionals compete with other factors that influence the policymaking process as well.

The same holds true for strategic warning analysis. A grounding of history may serve as the point of departure for assessing threats, such as North Korean missile launches, international terrorism, or a resurgent Russia or China. The mere provision of strategic warnings to the policymaker, however, is

8 Jack Davis, "The Kent Kendall Debate of 1949," *Studies in Intelligence* 36, no. 5 (1992): 92–103, accessed 25, 2017, https://www.hsdl.org/?view&did=3593. Davis provided excellent insight and perspective into the differences that shaped Sherman Kent's versus Willmoore Kendall's views on intelligence and the appropriate relationship with policymakers.

9 Amy Zegart, *Flawed by Design: The Evolution of the CIA, JCS, and NSC* (Stanford, CA: Stanford University Press, 1999). Professor Zegart examines the US intelligence community by evaluating the political forces that shaped the development of the community itself in order to evaluate why there are systemic failures.

insufficient if they do not translate into clear and decisive measures to mitigate the nature of the threat. The effectiveness of a warning system is also diminished if it is a result of a process that is designed to water down assessments with ambiguous language—again, harkening back to Zegart's assertion about the community itself.

The challenge to the intelligence professional is tied to this two-fold framework. This challenge is further compounded in the present as the US intelligence community faces an increasingly agile and diverse global threat. As such, the intelligence professional must be cognizant of the issues and cases of the past to determine their applicability and efficacy for future events and scenarios. As Thucydides suggested, however, those of us in the present tend to romanticize the past. While stories are important to imparting knowledge and ideals, the intelligence professional's knowledge of the past must be stripped of myth and folklore in order to understand the exact knowledge of events and how they can be applied in the future. The intelligence professional must also have exact knowledge of past cases in order to mitigate the use of quick analogies that many policymakers may adopt—again stemming from an imperfect knowledge of history.

Reflecting on history is necessary to understanding the future. That said, the study of history is not a mere recitation of facts, figures, and timelines. It leads to understanding the cultural and psychological nuances that constitute the environment. This holistic view of history grounds the intelligence analyst within the environment's narrative. To prepare for the future, the intelligence professional must evaluate past historical cases and trends to support three lines of inquiry:

- Re-examine the data and evidence.
- Evaluate the cases and trends within the context of history and causal cultural and psychological drivers.
- Assess the individual and organizational relationships involved.

Back to the Beginning: Reexamining Data and Evidence

Reexamining data and evidence, while seemingly a logical first step, is often one of the most overlooked aspects of intelligence analysis and the formulation of assumptions. Again, much of our knowledge of the past is based on prevailing assumptions and theories. In the study of conflict and warfare, however, there is new data and evidence that presents itself for evaluation. Much of this new information can contribute to the present understanding of how past events unfolded and how they contribute to decision-making. There is also data and evidence that is routinely declassified and made available to academics for further study and analysis. This serves as an excellent basis to reexamine some prevailing assumptions and myths of past events. A critical reexamination of data and evidence forces the intelligence professional to reexamine their prevailing assumptions and take a more objective view.

Despite the need to reevaluate data and evidence, many of the post-in-

telligence failure blue-ribbon commissions fail to objectively evaluate underlying data and evidence as a result of hindsight bias. As Erik Dahl explains, "Signals and warning that may have looked weak amid a sea of other data look strong and clear when viewed afterward and taken out of full context of the situation that intelligence analysts and policy-makers faced at the time."[10] He also notes that these commissions only evaluate past failures, but not successes. As a result, the perception of evaluation is skewed decidedly to one polarized side—that of failure. It is the responsibility of intelligence professionals in their reflections of history to dispassionately evaluate the data based on all perspectives—success, failure, peacetime, road to conflict, actual conflict, etc.

Contextual History: Evaluating Cases and Trends

This leads to the second line of inquiry—evaluating cases and trends within the context of history and causal cultural and psychological drivers. To engage in a strategic pause in the present while diplomatically attempting to contain an unstable despot does not necessarily equate to appeasement vis-à-vis Hitler's Germany in the 1930s. Analogies, while useful, are often misapplied, particularly when dealing within different historical periods or differences in culture or when lacking an appreciation for the unique psychological motivations within the context of the issue. The policymaker is challenged with evaluating a present situation, and analogies can prove useful, however, they can also have dire consequences. Similarly, understanding history and causal drivers to produce estimative intelligence is equally relevant to the intelligence professional—perhaps more so. The intelligence professional is held to a higher standard of evidence than the policymaker. The core function of the intelligence professional is to reduce the ambiguity of an intelligence problem. Understanding historical cases within the appropriate frame of perspective is critical when trying to apply it to a present situation.

This challenge is clearly emphasized by Heuer in his work, *Psychology of Intelligence Analysis,* where he states: "When an historical situation is deemed comparable to current circumstances, analysts use their understanding of the historical precedent to fill gaps in their understanding of the current situation. Unknown elements of the present are assumed to be the same as known elements of the historical precedent."[11] It is the responsibility of the intelligence professional to guard against these unknown elements and blind spots—particularly when applying a past case to a present circumstance. This can only be achieved by understanding and evaluating past cases, appreciating one's own cognitive biases, and critically evaluat-

10 Erik J. Dahl, *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond* (Washington, DC: Georgetown University Press, 2013), 15.

11 Richard J. Heuer, Jr., *The Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, 1999), 38.

ing the present circumstances for their potential relevance to a past case. The work of Neustadt and May is integral for both the policymaker and the intelligence professional in this case.[12]

Historical Actors: Individuals and Organizations

Lastly, the intelligence professional needs to understand how history plays in the assessment of individuals as historical actors and the organizations involved in the historical case. Past events, circumstances, individual and organizational relationships, the underlying culture, psychological drivers, and indeed even the language used to describe past events require a diachronic perspective of history. Kent refers to the character of individuals, groupings, and systems and the interplay that results between these actors as a fundamental premise to establishing understanding and knowledge.[13] As a wise person once said: "Everything changes and nothing stands still."[14] Past events, if they are to be interpreted for their present relevance, must be grounded with an understanding of history, its cultural and psychological context, and the relationship that existed between the actors and organizations involved. There is no substitute.

A grounding in history is essential to understanding the nature of strategic warning intelligence. In the words of Cynthia Grabo: "A knowledge of history, precedent and doctrine is extremely useful in assessing probabilities; and the citing of such precedents not only may bolster a case but also may tend to make the timid more willing to come to positive judgments."[15] It is this grasp of history and an understanding of the facts and evidence within a cultural and psychological context that contributes to the intelligence professional's ability to make their case before the policymaker. A superficial appreciation of history will not suffice, but a deeper understanding of history, culture, psychology, and the supporting data and evidence allows the intelligence professional to render a critical evaluation of the present circumstances while drawing upon the relevant lessons from the past.

While recognizing that a grounding in history is not a panacea for effective intelligence, it is important to recognize some of history's limitations. As referenced throughout, we possess an imperfect knowledge of the past. This is why it is imperative that we reexamine the underlying data and evidence to reassess our assumptions. Additionally, a superficial understanding of history without a deeper appreciation for cul-

12 Richard Neustadt and Ernest R. May, *Thinking in Time: The Uses of History for Decision-Makers* (New York: Simon & Schuster, 1986). Neustadt and May illustrate how particular historical models shape decision-makers. In other words, how decision-makers apply historical analogies unknowingly.

13 Kent, *Strategic Intelligence for American World Policy,* 6.

14 Plato, *Plato in Twelve Volumes*, trans. Harold N. Fowler (Cambridge, MA: Harvard University Press, 1921), 402a. Socrates attributes the quote to Heraclitus, an early Greek philosopher.

15 Grabo, *Anticipating Surprise,* 13.

ture will lead to flawed assumptions. An appreciation of context, culture, and psychology matters. This is Mansoor's premise of General Westmoreland as opposed to General Petraeus.[16] The need to develop cultural intelligence is vital. Lastly, we need to recognize that gaps in knowledge will always exist. Historical accounts are imperfect and the evaluation of the same data and evidence can lead to differing views. To presume we possess complete knowledge, especially given our reliance on our technology and data, is fallacious and places the intelligence professional at risk of making erroneous conclusions.

Conclusion

The reflections of history directly contribute to the ability of the intelligence professional to assess the present. Understanding the historical narrative informs an appreciation of the environment, culture, and underlying psychology. Even with its limitations, history provides the intelligence professional with the basis of assessing the future. An appreciation of history, however, cannot result in citing mere facts and figures. The intelligence professional must doggedly pursue three lines of inquiry. They must aggressively pursue the reexamining data and evidence to revalidate their assumptions. They have to evaluate past cases and trends within the context of history and an understanding of the underlying cultural and psychological drivers. Lastly, they must be able to assess individual and organizational relationships within the context of change in history. Focusing on these lines of inquiry, coupled with deeper knowledge of history, can vastly contribute to the imperfect art and science of intelligence analysis and assessing the future.

Jim Burch holds a Doctorate of Management (DM) and an MA in Military History. His primary area of research includes domestic intelligence issues in the post 9/11 era, the organizational design of the U.S. Intelligence Community, strategic warning analysis and the impact of technology on intelligence activities. Highlights from his research include the role of psychology between the intelligence professional and the policy-maker to convey warning and the impact of organizational culture in the intelligence community. He welcomes opportunities for continued research and collaboration.
jburch@apus.edu

16 Peter R. Mansoor, *Surge: My Journey with General Petraeus and the Remaking of the Iraq War* (New Haven, CT: Yale University Press, 2013), 96. Mansoor contrasts Westmoreland's superficial knowledge of Vietnam based on his misunderstanding of Lartéguy's insights in *Les Centurions*, which focused largely on the Algerian as opposed to Vietnamese conflict.

References

Bar-Joseph, Uri. *The Watchmen Fell Asleep: The Surprise of Yom Kippur and Its Sources*. Albany, NY: The State University of New York Press, 2005.

Betts, Richard K. *Enemies of Intelligence: Knowledge and Power in American National Security*. New York: Columbia University Press, 2007.

Christianson, Erik. *Channeling the Past: Politicizing History in Postwar America*. Madison, WI: The University of Wisconsin Press, 2013.

Dahl, Erik J. *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond*. Washington, DC: Georgetown University Press, 2013.

Davis, Jack. "The Kent Kendall Debate of 1949." *Studies in Intelligence* 36, no. 5 (1992): 92–103.

Grabo, Cynthia M. *Anticipating Surprise: Analysis for Strategic Warning*. Washington, DC: Joint Military Intelligence College, 2002.

Heuer, Richard J., Jr. *The Psychology of Intelligence Analysis*. Washington, DC: Center for the Study of Intelligence, 1999.

May, Ernest R. *"Lessons" of the Past: The Use and Misuse of History in American Foreign Policy.* Oxford, England: Oxford University Press, 1975.

Neustadt, Richard and Ernest R. May. *Thinking in Time: The Uses of History for Decision-Makers*. New York: Simon & Schuster, 1986.

Plato. *Plato in Twelve Volumes*. Translated by Harold N. Fowler. Cambridge, MA: Harvard University Press, 1921.

Thucydides. *History of the Peloponnesian War*. Translated by Rex Warner. New York: Penguin Classics, 1978.

US Government, Intelligence Survey Group. *The Central Intelligence Agency and the National Organization for Intelligence: A Report to the National Security Council*. Washington, DC: Government Printing Office, 1949.

Wohlstetter, Roberta. *Pearl Harbor: Warning and Decision*. Stanford, CA: Stanford University Press, 1962.

Zegart, Amy. *Flawed by Design: The Evolution of the CIA, JCS, and NSC*. Stanford, CA: Stanford University Press, 1999.

An Interview with Emerson Brooking, the Co-Author of *LikeWar: The Weaponization of Social Media*

Conducted by Dr. Carter Matherly

Mr. Emerson Brooking is the co-author of the book *LikeWar: The Weaponization of Social Media*. The book not only highlights how other nations have taken offensive maneuvers using social media, but also managed to move past traditional psyops and employ psychology as a warfighting domain in its own right. Mr. Brooking's work continues today as he maps the battlespace in this emergent domain. For an in-depth review of *LikeWar,* please see the book review in this volume by Austin Gouldsmith. To see more of Mr. Brooking's current work and access some fantastic datasets, visit his repository on GitHub, https://github.com/DFRLab/Dichotomies-of-Disinformation.

CM: There has been significant discussion concerning kinetic versus non-kinetic operations as core concepts for effects-based operations. How do these terms, and associated perspectives of targeting, apply to planning and execution in the psychological domain?

EB: Effects-based targeting *must* take primacy in the planning and execution of operations in the psychological domain. One must be familiar with an adversary's key capabilities and weaknesses that information warfare specialists can most readily exploit. As much as possible, this strategic determination should be made in advance, before conflict begins.

Once an information conflict is underway, it is too late to conduct much deliberate, effects-based planning. This is because of the speed with which such conflict takes place, and the fact that it is very much driven by the opportunism and initiative of individual operators. If these operators have received clear, effects-based guidance, they can orient their efforts appropriately.

CM: Psychological warfare and MISO are not new concepts; however, technology has breathed new life into these age-old ideas. What are some of your most notable observations from this transformation? What do you find most challenging about emerging technologies (e.g., deep fakes)?

EB: The major revolution that the modern internet has brought to psychological warfare and military information

 doi: 10.18278/gsis.5.1.8

support operations is that of asymmetry. Thanks to the widespread availability of social media platforms, even a resource-poor adversary can conduct sophisticated propaganda and influence operations at a very low cost. At the same time, highly resourced organizations struggle to respond effectively to these efforts. They are stymied by bureaucratic limitations and the fact that, quite often, acknowledging an adversary's influence efforts only expands their reach.

There have been numerous other technical innovations—notably, advancements in neural networks and the development of "deep fakes"—that may increase the persuasive effect of psychological operations at the margins. But in the end, I believe it comes back to the extraordinary cheapness and accessibility of these capabilities.

CM: If you were to create a US "digital army" how would you do it? What would be your approach to organization?

EB: I would delineate clear responsibilities between units. Most particularly, in order to abide by US laws and norms regarding psychological operations, I would focus most of our efforts on force protection. We should resist the temptation to militarize US public diplomacy.

I would also ensure that as much authority as possible was devolved to individual operators within the US "digital army." Effective psychological operations require a degree of flexibility and creativity that is often at odds with military organization. If this freedom were not forthcoming, the digital army would not be able to fulfill its mandate.

CM: What key skillsets do you see as vital to members of that "digital army" for both offensive and defensive actions? What training do you think is most important to the evolution of an Information Operations Operator?

EB: Anyone involved in psychological or military information support operations should be adaptable, entrepreneurial, and—above all—creative. It requires a unique skillset to find and exploit opportunities in a fast-moving narrative battle. Such operators would need to be as familiar with the principles of viral marketing and consumer psychology as they were with the principles of military strategic communications.

CM: In general, what are your thoughts on how warfighters can use the psychological domain to help bridge the gap between intel and operations?

EB: The right message, targeted in the right way and propelled in the right manner, can cause an adversary to make missteps that can immediately be exploited by intelligence-gatherers. In some cases, the message may obviate the need for a kinetic confrontation entirely.

CM: You both are working on some pretty exciting upcoming projects. Could you tell our readers about them and their importance to the psychological domain?

EB: I have been hard at work mapping the constituent elements of what I call "political disinformation campaigns"—psychological operations by another name. We now have thousands of examples of such operations unfolding all around the world, being directed toward a variety of military and political ends. By mapping these campaigns and assessing them in aggregate, I hope to draw out new lessons about the ongoing information revolution.

In recent weeks, my organization—the Digital Forensic Research Lab of the Atlantic Council—has also been focused on tracking dis- and misinformation regarding the coronavirus pandemic. Russia, China, and the United States have each been involved in significant influence efforts to shape global perceptions of the pandemic. The outcome of this narrative battle will affect global politics for many years to come.

Contesting the Psychological Domain during Great Power Competition

Jeremiah Deibler

The views expressed are those of the author and do not necessarily reflect the official policy or position of the Department of the Air Force, Department of Defense, or the United States Government.

It is comparatively insignificant but nonetheless relevant to discuss Great Power Competition in the wake of the coronavirus (COVID-19) crisis. Despite the need for global cooperation amid the COVID-19 pandemic, elements of Great Power Competition persist. In early March, Lily Kuo, a Hong Kong correspondent for the *Guardian*, detailed the Communist Party of China's (CPC) and Chinese state media's alternative narrative, which sowed seeds of doubt about COVID-19's origination in China.[1] The CPC, according to Kuo, seized on comments by Robert Redfield, the director of the US Centers for Disease Control and Prevention (CDC).[2] Exploiting Redfield's inconclusive language, Spokesperson and Deputy General of the Foreign Ministry's Information Department Lijian Zhao shared the video clip multiple times and speculated:

> CDC was caught on the spot. When did patient zero begin in US? How many people are infected? What are the names of the hospitals? It might be US army who brought the epidemic to Wuhan. Be transparent! Make public your data! US owe us an explanation![3]

Shortly thereafter, the United States' political leadership, including President Donald Trump, modified its language to publicly call COVID-19 the Chinese virus. Jabin Botsford, staff photographer at the *Washington Post*, identified modifications by the President to shape the informational environment.[4]

The exchange between the CPC and American national security leadership is intrinsically linked to the ongoing competition between emergent (China) and existing (US) great powers. China is seizing the opportunity to lead the global response to COVID-19 as it seeks to become the preferred partner for the international community. The phrase "preferred partner" is the operative concept behind competition. In a shift from phase-based planning to

 doi: 10.18278/gsis.5.1.9

the conflict continuum, within the US Department of Defense (DOD) vernacular, there has been much ado about competition. How is it defined? What does it look like? What are the subsequent implications for how the DOD does business? The purpose of this paper is to (1) identify key characteristics of Great Power Competition, (2) review the impacts of these characteristics on the military instrument of power, and (3) make recommendations for planners and intelligence organizations and professionals supporting the Joint Forces Commander (JFC).

Figure 1. @jabinbotsford captured presidential information power.[5]

The Characteristics of Great Power Competition

Much has been said about competition since it was discussed by Secretary of Defense (SecDef) James Mattis in the lead-up to his publication of the National Defense Strategy (NDS) in 2018. The NDS informed an updated Joint Publication (JP) 3-0, which presented the concept of the Conflict Continuum (see Figure 2). Figure 2 clearly shows the interrelationship between national instruments of power (IOP) across the continuum. Specifically, during cooperation and competition, military engagement, security cooperation, and deterrence serve to keep geopolitical relationships in the desired state of cooperation or competition. Crisis response and limited contingency operations serve as emergency actions to use IOPs to prevent escalation to destructive large-scale combat operations. Cooperation and competition are fundamentally about building and cultivating relationships.

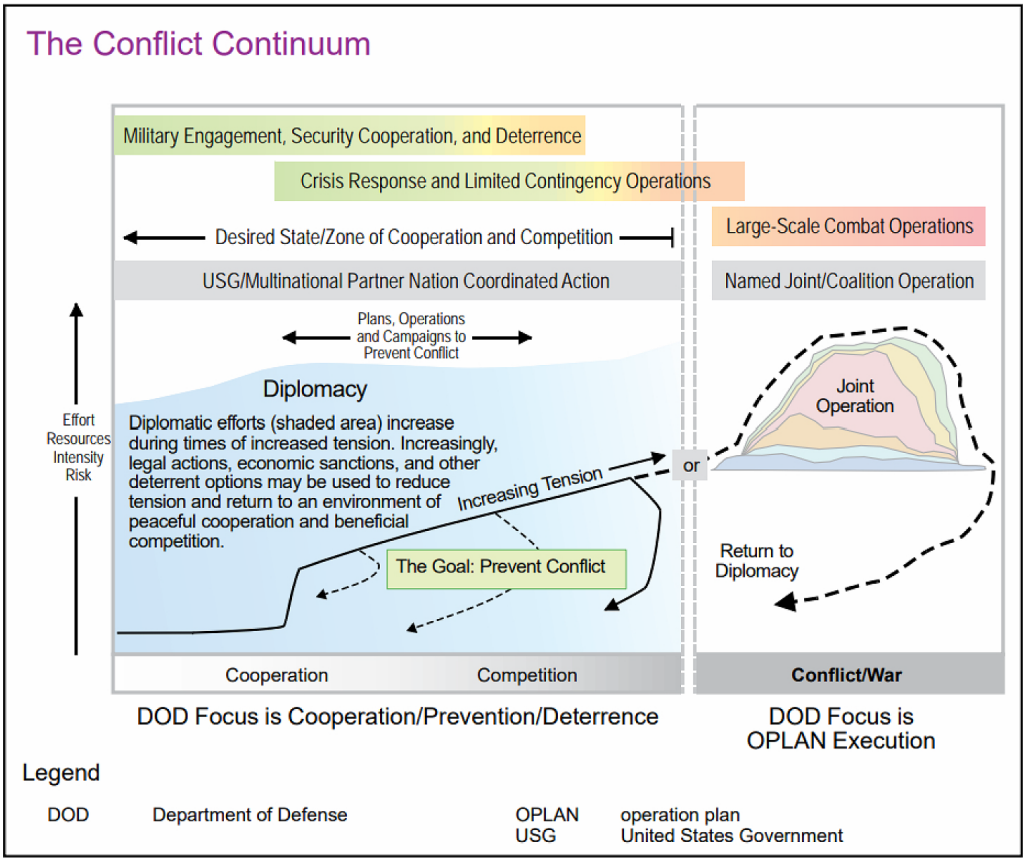


Figure 2. Conflict continuum.[6]

Between the fall of the Soviet Union (USSR) in 1991 and roughly 2012, the US existed in a unipolar international environment that offered it the opportunity to dictate the terms of most international relationships. It combined its comparative national power with a comprehensive set of strong alliances and international organizations, presenting unparalleled global leadership under the Bretton Woods liberal world order. In 1989, prior to the official fall of the USSR, Francis Fukuyama famously published his article called "The End of History?," claiming that "The triumph of the West ... is evident first of all in the total exhaustion of viable systematic alternatives to Western liberalism."[7]

Absent any other choice for a preferred partner, non-powers were either a part of the US-led international system or existed outside of the system and therefore were at a comparative disadvantage. In 2018, Fukuyama published a new book, *Identify: The Demand for Dignity and the Politics of Resentment.* Louis Menand summarizes Fukuyama's argument: that the "contemporary dissatisfactions" of "Vladimir Putin, Osama bin Laden, Xi Jinping" and even national movements like "Black Lives Matter" and "#MeToo"

were antitheses to the "global liberal world order" and as a result, "liberal democracy and free trade may actually be rather fragile achievements."[8]

In the last decade, regional and global alternatives emerged. Iran leads proxy conflicts across the Middle East. Its leader and strategist was killed by a US strike this year.[9] Russia exploited the proverbial ethnic domain in order to annex Crimea.[10] China increased its global diplomatic and economic activities through the Belt Road Initiative (BRI).[11] In the 2018 NDS, Secretary Mattis referred to these actors as "revisionist powers and rogue regimes."[12] The key take away is the idea of choice. To a certain extent, market dynamics have taken hold in the geopolitical environment. For the better part of the transitional period between the twentieth and twenty-first centuries, the US-led global world order was the only option. The first characteristic of Great Power Competition that we must bear in mind is the interplay between rational choice and market dynamics on the geopolitical plane.

President Rodrigo Duterte of the Philippines provided, perhaps, the best commentary on geopolitical market dynamics and non-powers' rational choice: "[The US creates] rules and norms for almost everyone, and some refuse to be bound by the same ... [The US and its allies] weaponize human rights oblivious to its damaging consequences."[13] Regardless of whether President Duterte's perception of critical human rights is accurate, the implications for the geopolitical marketplace are clear. President Duterte now has a choice. His near neighbor, China, is closer than and, arguably, possesses comparative national power to the US. Further, China is now offering an alternative to the US world order. In July 2016, as part of a speech commemorating the ninety-fifth anniversary of the founding of the CPC, President Xi Jinping declared his nation's "commitment to an independent foreign policy ... on the basis of the Five Principles of Peaceful Coexistence."[14]

Xi Jinping's Five Principles of Peaceful Coexistence

- Mutual respect for each other's territorial integrity and sovereignty
- Mutual non-aggression
- Mutual non-interference in each other's internal affairs
- Equality and cooperation for mutual benefit
- Peaceful coexistence

Figure 3. President Xi Jinping's Five Principles for Peaceful Coexistence.[15]

Certainly, "mutual non-interference" resonates with President Duterte's message above. This does not mean that President Duterte will immediately align himself with China; however, it gives him leverage in negotiating with the US. The geopolitical marketplace forces the Great Powers into weaker

negotiating positions with strategically located nations.

Part of President Duterte's and other leaders' rational calculus is the comparative military power and its associated threat and implied national risk. Nowhere is this more evident than in Australia. A partner within the Five-Eyes intelligence alliance with the US, Canada, United Kingdom, and New Zealand, Australia faces a complex position in the Great Power Competition security environment. On the one hand, as Philip Citowicki argues, "Australia is acutely aware that supporting the fragile democracies of the Pacific requires greater cooperation with like-minded nations."[16] On the other hand, Tom Hanson suggests that, due to significant "Chinese capital investment" in key sectors "from port facilities to infant formula to commercial real estate to agriculture," Australia may be at risk of having "to choose between deepening its economic relationship with [China] and its longstanding alliance with the United States."[17] The truth is likely somewhere in between, but the shift toward a world shaped by Great Power Competition places the Australian government in a complex position. In these situations, traditional allies are more likely to come into geopolitical friction. When tensions rise, a decision is made regarding actions taken to protect national interests. Depending on the level of national interest, traditional allies may transition from cooperation to competition or conflict.

National interest was characterized by Donald Nuechterlein in his essay "National Interest and Foreign Policy: A Conceptual Framework for Analysis and Decision-Making" in the *British Journal of International Studies* in 1976 (Figure 4).

Level	Description
Survival	The very existence of a nation-state is in jeopardy as a result of overt military attack on its own territory or from the threat of attack if an enemy's demands are rejected.
Vital	Serious harm will very likely result to the state unless strong measures, including the use of conventional military forces, are employed to counter an adverse action by another state or to deter it from undertaking a serious provocation.
Major	The political, economic and ideological wellbeing of the state may be adversely affected by events and trends in the international environment and thus requires corrective action in order to prevent them from becoming serious threats (vital issues).
Peripheral	The wellbeing of the state is not adversely affected by events or trends abroad, but the interests of private citizens and companies operating in other countries might be endangered.

Figure 4. Nuechterlein's levels of national interest.

Nuechterlein's construct suggests that the only justification for going to conflict is over survival or vital national interests. However, it is arguable that for much of the period prior to the resurgence of Great Power Competition, much of the conflict that the US participated in was for major to peripheral na-

tional interests. For US decision-makers, the risk to the homeland and its forces did not meet the threshold that warranted a pause in action. This is not to criticize those decisions, but rather to highlight the calculus that a unipolar world affords a Great Power. This willingness to breach the threshold of conflict can be viewed alternatively as a decision-maker's band of tolerance. Amanda Donnelly details the band of tolerance in relation to strategic response options (SRO) in her thesis at the School of Advanced Air and Space Studies. Based on Jeffrey Reilly's lectures from the Multi-Domain Operational Strategist program at Air University's Air Command and Staff College, the band of tolerance (Figure 5) represents the area of options within which the decision-maker is willing to accept SROs.[18]

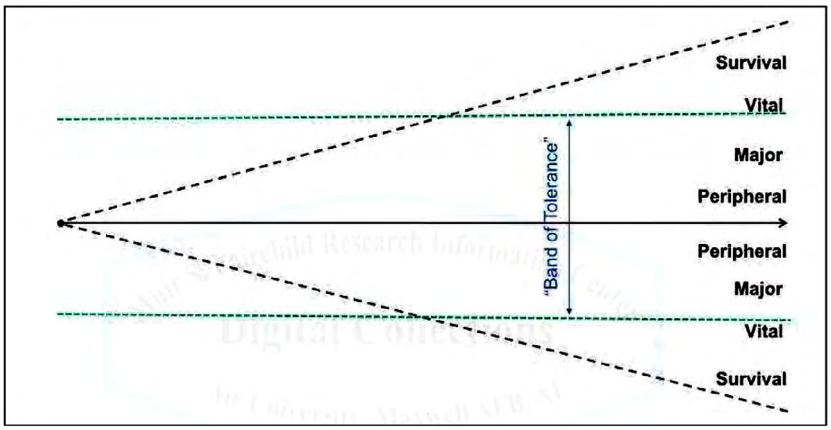


Figure 5. Band of tolerance.

More critical for the purposes of this paper is the impact of comparative national power on the band of tolerance for decision-makers. In short, as the comparative national power between two nations becomes higher and closer, the cost and therefore the risk become significantly higher. As risk rises, the band of tolerance shrinks until nations are unwilling to transition from competition to conflict for anything but the most vital national interests and survival. Therefore, whereas the US may be more willing to put pressure on President Duterte in a unipolar world to more fully comply with human rights, it may jeopardize the national interests of a higher order in the era of Great Power Competition. The national interests remain, including peripheral interests, but the desire to proceed to destructive force at the risk of escalation reduces significantly.

It is the combination of the geopolitical marketplace and the rising risk's impact on the band of tolerance that produces the third key characteristic of Great Power Competition: gray zone tactics or warfare. In high-risk security environments, activities below the threshold of conflict naturally be-

come the priority mechanism. As Secretary Mattis laid out in the NDS:

> Both revisionist powers and rogue regimes are competing across all dimensions of power. They have increased efforts short of armed conflict by expanding coercion to new fronts, violating principles of sovereignty, exploiting ambiguity, and deliberately blurring the lines between civil and military goals.[19]

Multiple actors employ gray zone tactics today. The US House Intelligence Community summarized Robert Mueller's report on Russia's social media warfare.[20] In his article in *MIT's Technology Review,* Vince Beiser details the expanse of China's dredging operations, including both the South China Sea (SCS) and multiple BRI projects (see Figure 6).[21] The Center of Strategic and International Studies' (CSIS) Asia Maritime Transparency Initiative (AMTI) monitors and evaluates Chinese Maritime Militia activities within the SCS in international or non-Chinese territorial waters.[22]

Figure 6. The Wan Qing Sha dredging in the vicinity of Colombo, Sri Lanka.[23]

In many of these cases, there is no clear breach of either President Putin's or President Xi's band of tolerance. Most importantly, it also does not cross the threshold for President Trump. Gray zone tactics account for the geopolitical marketplace and both decision-makers' and their opponents' risk calculus to achieve policy objectives without risking the transition to conflict. These concepts are by no means new in human history. Christopher Andrew and Vasili Mitrokhin published an excellent book, *The World was Going our Way: The KGB and the Battle for the Third World*, on the history of Soviet Union active measures across the globe during the Cold War. The introduction of their book

references Vladimir Lenin's fiery speech on the Russian Revolution in 1917. Lenin opined: "In the coming battles of the world revolution, this movement of the majority of the world's population, originally aimed at national liberation, will turn against capitalism and imperialism."[24]

The Soviet Union may have fallen in 1991 but it was not the end of history. Great Power Competition is here. The American national security apparatus should remain cognizant of the characteristics of that global environment: (1) the world is a geopolitical marketplace and we now have competitors who offer alternatives to rational actors, (2) the mounting costs of any conflict reduces the likelihood of the transition to conflict but does not eliminate it, and (3) the predominate tactic is gray zone warfare.

Great Power Competitions Implications and National Security

In a unipolar world, the comparative strength of the US military and its allies is effectively insurmountable when faced with a conventional threat. Consider the emergence of the Islamic State in Iraq and Syria (ISIS). According to the Wilson Center's timeline of events, the transition from conventional offensives to asymmetric tactics is clear. In June 2014, ISIS employed conventional maneuvers in order to seize Mosul; however, the emergence of US strikes and Peshmerga-US cooperation necessitated ISIS's transition to asymmetric tactics by the end of the year.[25] The US military advantage allowed the US national security apparatus to lean heavily on the military as the supported instrument. This orientation is manifest in the structure of the National Security Council.

Within IOPs, the DOD is the 800-pound gorilla, comprising three of the statutory seats compared to one each for diplomacy and economics.[26] Information is notably absent, although many would align the IOP to the President or Secretary of State. Nonetheless, it is clear why the national security apparatus is a threat-oriented culture. At the apex of global hegemony and a unipolar world, a national security strategy inherently seeks to maintain the status quo. As a result, any effort to revise the structure of the world order is viewed as a threat. This is not to be dismissive of the challenges that the CPC, the Putin regime, and other disruptive actors present. Rather, it serves as a frame of reference for US national security culture, its associated vulnerabilities, and where the military might shift its approach accounting for the characteristics of Great Power Competition.

A threat-oriented culture seeks to anticipate and prepare for conflict, as it should. However, a threat-oriented culture trends towards denouncing bad faith actors rather than offering a more attractive alternative. In comparison, a diplomacy-centric national security apparatus focuses on "build[ing] and sustaining[ing] relationships."[27] On the other hand, an economic-centric approach seeks to maximize economic

growth to "create wealth for Americans and our allies and partners."[28] Both take a more positive rather than negative orientation towards potential partners.

An information-centric national security strategy is unclear but can be gleaned from the US National Security Strategy (NSS) published by the President in 2017. The NSS denounced "American competitors [who] weaponize information to attack the values and institutions that underpin free societies, while shielding themselves from outside information."[29] By extrapolating the threat posed by malign actors within the information sphere, it is possible to consider an information-centric posture. It requires a coherent strategic narrative that is consistently supported by the actions of other IOPs.

Suppose the US national security strategy shifted towards an information-centric approach. Information-centric does not imply that diplomatic, economic, and military actions disappear from the toolkit, nor does it dismiss the concept of a threat. Rather, an information-centric national security strategy, first and foremost, considers how each of those actions support or detract from its strategic narrative.

Information-Centric National Security Strategy and the Military Instrument of Power

What does this mean for the DOD and, as a result, the military? The is no better modern example of the military supporting an information-centric strategy than the strikes against Syria chemical warfare sites in 2018. Within minutes of executing the strikes, Secretary Mattis hosted a press conference where he invoked international norms and standards while offering CJCS General Dunford a chance to articulate the strike's purpose:

> The strike was not only a strong message to the regime that their actions were inexcusable, but it also inflicted maximum damage, without unnecessary risk to innocent civilians.[30]

Further, in a show of solidarity, the French and British attachés were present and participated in the airstrikes. In short, leading the narrative rather than reacting is critical. Today, malign actors lead the narrative and the US national security apparatus reacts. The military must adjust its approach to this environment by shifting from system-centric warfare to message-centric warfare. This is especially evident in the Air Force, where the system-centric approach to warfare remains supreme.

During the Gulf War, John Warden first proved the application of Centers of Gravity (COG) analysis and the system-centric approach to warfare, referred to as Effects-Based Operations (EBO). Yet, ironically, the Gulf War is an excellent example of effective message-centric warfare. In fact, it sparked an after-action debate that is relevant today. It began with none other than NDS author and recent SecDef James

Mattis. As then-General Mattis, Commander of Joint Forces Command, he fired a shot across the bow of the Air Force's new sacred cow: EBO.[31] To be fair to General Mattis, his argument against EBO was not necessarily that it was ineffective, but rather that it could not be overly applied. Within the article, General Mattis conceded that "Elements of [EBO's] concepts have proven useful in addressing 'closed systems,' such as targeting, where effects can be measured per the U.S. Air Force's deliberate analysis and targeting methods."[32]

Against Iraq's Kari Integrated Air Defense System (IADS), John Warden's approach was wildly effective. Kari IADS was tailor-made for a scientific approach to EBO. As Michael Gordon and General Bernard Trainor describe it in *The General's War,* "Like spokes of a wagon wheel, the Intercept Operations Centers … led to regional Sector Operations Centers (SOC)."[33] In theory, if you break the right nodes (critical elements), you destroy the system. However, in the conflict's undercurrent, "the first 48 hours of the Gulf War showed beyond a doubt that electronic warfare technologies could keep US servicemen safe from enemy fire by denying the enemy the use of his command, control, communications and intelligence."[34] Much like German strategic bombing enhanced the effectiveness of its ground offensive at Guernica during the Spanish Civil War, Electronic Warfare (EW) and Information Operations (IO) enhanced the effectiveness of air strikes against Kari IADS. The IO and EW campaigns during the Gulf War were effective precisely because they were synchronized with the targeted strikes against system-critical nodes. John Warden's COG theory was proven correct. Yet, hidden in that lesson was the complementary role that military operations played in the broader strategic narrative.

Prior to the Gulf War, National Security Directive (NSD) 45, clearly stated the purpose of the effort: "This authorization is for the following purposes: to effect the immediate, complete and unconditional withdrawal of all Iraqi forces from Kuwait; to restore Kuwait's legitimate government; to protect the lives of American citizens abroad; and to promote the security and stability of the Persian Gulf."[35] President Bush achieved coherence in his message. On August 8, 1990, with clear language to both the American people but also to Saddam Hussein, President Bush restated the above principles.[36] He achieved consistency and clarity. The military actions from there, including air strikes, supported this message, albeit from the operational level.

This conflict is critically important in the context today. The message's coherence, clarity, and consistency remained paramount. Consistency also applied to the actions taken by the US military in support of that message. The pamphlets below were dropped in support of military action and clearly restated the message for Iraqi troops in order to circumvent Iraqi propaganda (Figure 7).[37]

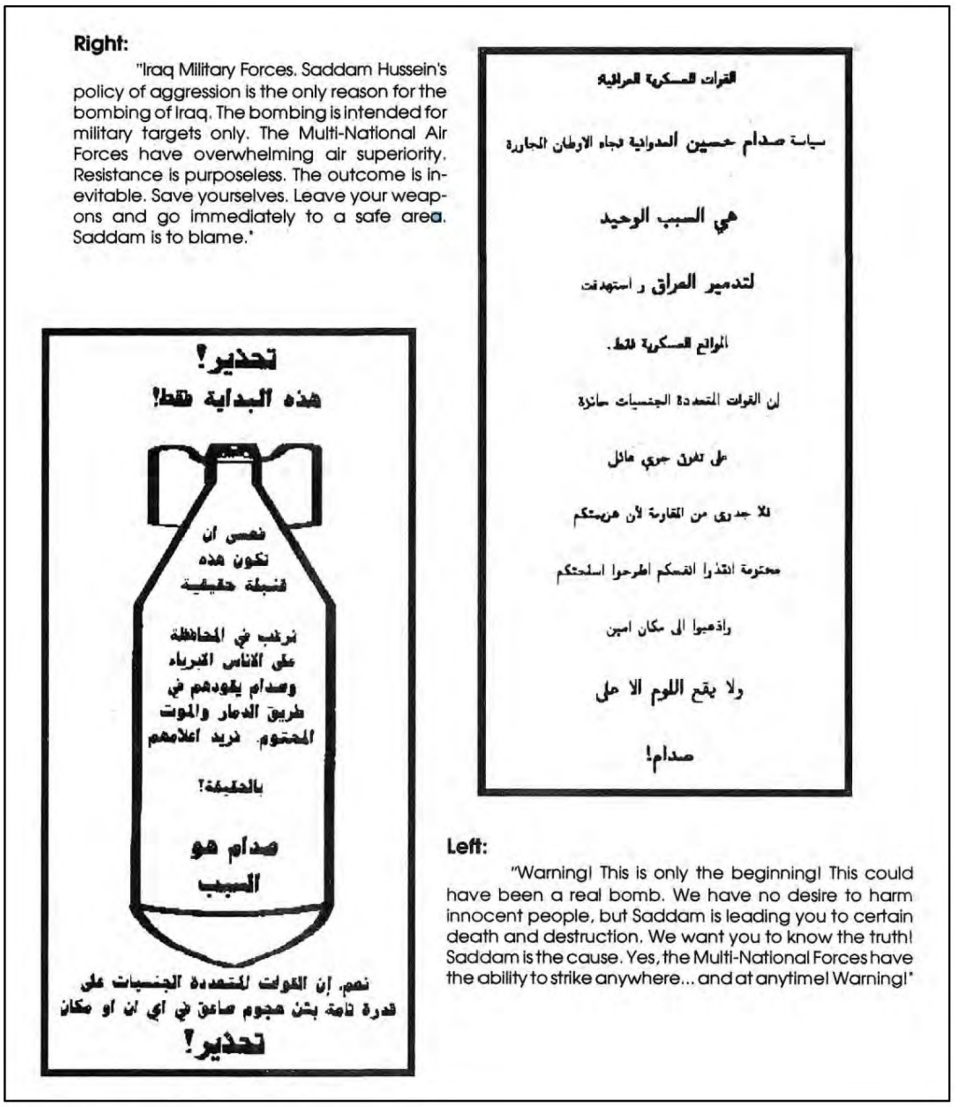


Figure 7. Leaflets from the Gulf War.[38]

Military operations in the era of Great Power Competition must similarly support the strategic message by modernizing their approach to social media and other modern information dissemination mechanisms. The Internet Research Agency in Russia and China's recent surge on Twitter after the Hong Kong protests are evidence of the resurgent powers' understanding of this sphere.

For Russia and China, the Gulf War is a critical study and impacts both nations' military modernization efforts. In *Unrestricted Warfare*, Colonels Qiao Liang and Wang Xiangsui explore American military doctrine through the lens of Desert Storm, Somalia, and Bosnia in order to identify the future direction of warfare. Published in 1999, these military theorists identified the root strength of US military power as

not that of "individual systems" but the "systemization" or integration of the systems to afford information sharing and synchronization.[39]

In summarizing Ronald R. Luman's arguments regarding unrestricted warfare, the RAND Corporation suggests that "nation-states (and non-state) actors are now more likely to use any and all measures short of war available to achieve their strategic objectives."[40] Colonels Qiao and Wang emphasize an emergent (in 1999) revolution, where weapons are less about "gunpowder" and more about "information."[41]

Rather than "fight the fight with that fits ones weapons," the Colonels argue the US "[built] the weapons to fight the fight," potentially exposing the US to a fight they did not anticipate.[42] By watching the US fight the same war across a decade with the same tactics and the same narrow view of war, they implied the need for a national security apparatus to fight a fight for which the US had not built its force. In that fight, the first blow may not be one of traditional military physical power, but rather "a single man-made stock-market crash, a single computer virus invasion, or a single rumor or scandal that results in a fluctuation in the enemy country's exchange rates or exposes the leaders of an enemy country on the Internet."[43] Today, China, Russia, Iran, and other actors practice the Colonels' unrestricted warfare as gray zone tactics below the threshold of warfare.

By avoiding the strength and exploiting the weaknesses of military IOP, China and Russia achieve policy objectives with little friction. Russia and China modernized its force to own the electromagnetic spectrum (EMS); accessing EMS is a precondition for communicating when projecting forces into theater.[44] They, and other actors, complemented these efforts by building advanced Anti-Access, Area Denial (A2AD) systems.[45] Further, Russia and Iran seek to follow China's lead to close off their internet from the global community.[46] Thus, from an offensive approach, the typical US military transition to conflict is significantly more difficult than it was during Desert Storm. Military analysts like Colonels Qiao and Wang spent decades studying our approach and their policymakers listened. Ultimately, they developed a defensive strategy that exploits the greatest vulnerabilities in our way of war. In short, the US needs a different operational approach.

Message-centric operations are a potential methodological shift towards the US operational approach. It necessarily requires that, in the geopolitical marketplace, commanders re persistently having conversations with other decision-makers both through words and actions. Rather than an end-state, commanders instead present a clear, concise, and coherent strategic narrative that all subsequent actions must support. This operational approach more effectively aligns with Great Power Competition along the continuum where military engagement, security cooperation, deterrence, crisis response, and when necessary, limited contingency operations are the prima-

ry scope of military efforts. Rather than focusing on end-states, it asks several key questions. What do I mean to say? Who am I saying it to? Does the message say what I intend? How is it being received? Absent methodological testing, it is safe to hypothesize that this approach would more readily arm commanders with the ability to function in Great Power Competition to deal with the baseline question: was my message sent and was it received?

Consider the introduction and the narrative scuffle between the CPC and US national security leadership over COVID-19. In the context of unrestricted warfare, it is critical to the CPC to gain positioning within the global leadership race. Similarly, it is critical for the US to maintain its place as a global leader. The tit-for-tat messaging that took place was a subordinate argument to the broader fight. What was each nation's broader message? What other actions took place to complement the broader message? Who was the target audience for the messaging by the CPC or by US national security leadership?

This paper will not evaluate these questions pertaining to COVID-19. Instead, it shows how for military IOP in Great Power Competition, the message is, perhaps, more important than the ability to attrite adversarial forces to gain military advantage. China, Russia, and other actors studied the US military for decades and discovered vulnerabilities in its way of war. As a result, they have tailored their approach to geopolitical conflict by remaining below the threshold of conflict through unrestricted warfare and gray zone tactics. Given the risk to forces upon transition to conflict, it is unlikely that there will be a transition from competition to conflict. As a result, it may be more advantageous for commanders to adopt a message-centric approach to operations when conducting military engagement, security cooperation, deterrence, crisis response, and, when necessary, limited contingency operations. If this is the approach that commanders take, the following sections suggest two evolutionary and one disruptive approach to the US operational approach, scoped specifically to the psychological domain. First, the paper discusses characteristics and implications of the psychological domain on narrative, and then provides three recommendations.

Message-Centric Operations and the Psychological Domain

In a previous article for the *Over-the-Horizon (OTH) Journal*, I laid out my perspective on the Air Force's approach to information warfare (IW) in the wake of the establishment of a new IW numbered Air Force. In it, I argue for doctrinal and organizational design elements to engage in a tactical information fight between two air component commanders.[47] Specifically, I employ a model of a command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) developed by the Research and Development (RAND) Corporation (See Figure 8.)

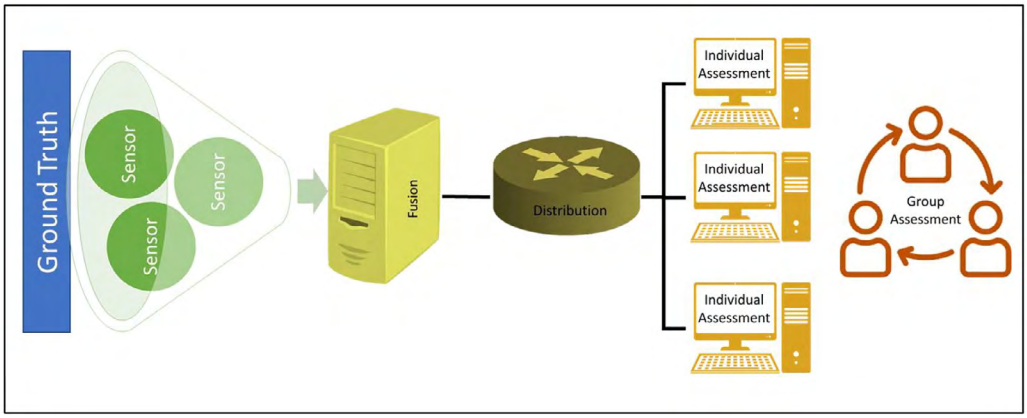


Figure 8. Author's depiction of RAND's C4ISR model.[48]

I do not intend to rehash my arguments from that paper here. In this article, I leverage the same C4ISR model to focus on two specific steps: (1) individual assessment and (2) group assessment. RAND describes the steps as follows:

- Individual Assessment. Each user then attempts to interpret the [environment] he has received to achieve some level of realization of the battlespace.[49]

- Group Assessment. The users then collaborate with each other in an attempt to improve their realization of ground truth in the battlespace. This report models the effectiveness of collaboration as a function of the skills of the users and the collaborative group as a whole but does not examine the [effects] of the network's communications tools on collaboration.[50]

In order to effectively scope the conversation about message-centric warfare to the psychological domain, it is critical then to consider individual and group psychology. It is the span across the individual's interpretation, the group's collaboration, and the decision-maker's action that the psychological domain occurs in two parts: first, cognitively, and second, behaviorally. The cognitive component is heavily dependent on attention, which shapes observation. Once an event gains attention, it is blurred by individual or group biases. These biases are derived from historical experience and shape reaction to the perception of the environment.

To affect an adversary's cognitive system, any message or action must first gain attention. In his book, *Consciousness and the Brain*, Stanislas Dehaene discusses the inner workings of the brain, specifically the relationship between unconscious and conscious thought. Through rigorous experimentation and research, Dehaene concludes that conscious perception is limited to a single focus, yet is triggered by an observable electrical pulse that broadcasts information across the brain."[51] To summarize Dehaene: there is a trigger from unconscious observation to con-

scious observation, requiring whole brain analysis. In short, that trigger is attention. Attention, then, is a finite resource compared to the perpetual unconscious observation performed by the human observer. This resource is the primary avenue of approach for message-centric warfare. Peter Singer and Emerson Brooking, in *Like War*, detail the "key elements" that masters of social media warfare employ: "*narrative, emotion, authenticity, community, and inundation*."[52] These elements are the essence of message-centric warfare. Mastering these elements to seize and retain attention were critical for ISIS recruiting and Russian disinformation campaigns during the 2016 US election. Table 1 shows how Singer and Brooking define the key elements and their key characteristics:

Table 1. The Characteristics of the Key Elements Social Media Warfare.[53]

Element	Summarized Characteristics from *Like War*
Narrative	Enable individuals or large groups to turn complex environments into simple laws or principles for perceiving the world; consistent, simple, resonate with individual or group history; novelty by "subvert[ing]" a norm or expectation.
Emotion	"the stronger the emotions involved, the likelier something goes viral"; negative emotions spread faster and must be repeatedly evoked.
Authenticity	Establish and adhere to a brand; remain consistent even amid embarrassment or negative attention; use plain, common, relatable language
Community	People want to belong to something bigger than themselves; warmth; camaraderie; the idea matters less than connection; anti-isolation.
Inundation	Attention is a finite resource, it is possible to use up all the oxygen in the room; does not need to be direct action, may be indirect through proxies or unaffiliated advocates; data science and publicly available data may be exploited to more rapidly tailored attention-seeking messages.

The implication of Singer and Brooking's elements is that a consistent, emotive narrative that authentically evokes the target audience's shared cultural history is likely to outcompete other narratives in a finite attention environment. It may not necessarily shape behavior, but it can build a community around a shared perception of events that is reinforced by continual conditioning.

The relationship between consistency and conditioning in order to increase the probability of behavior is thoroughly explained by B.F. Skinner in *Science and Behavior*. At a basic level, a behavior is a reflex, which itself is response to a simulus.[54] Conditioning simply replaces the stimulus to trigger a desired behavior.[55] Example stimuli include attention or approval, which

Skinner also calls reinforcers.[56] The dopamine hits and associated reinforcement that comes with social media activity is well-documented. These reinforcers can be negative (deprivation) or positive (reward).[57] Consistent stimuli therefore reinforce any narrative and associated perceptions of new events. Conversely, a consistent narrative may serve as its own stimulus when complemented by the attention or approval received via social media. This applies to the operational environment as well.

Consider unsafe maneuvers in the air and at sea by Russian forces against US and North Atlantic Treaty Organization (NATO) assets. In June 2019, Russia first conducted a dangerous maneuver against a US spy aircraft.[58] A day later, The US Navy's Seventh Fleet reported an unsafe maneuver by a Russian Destroyer against a US Cruiser.[59] Two months later in August, NATO criticized Russian aircraft for "act[ing] in an 'unsafe manner'" against "two Spanish F-18[s]."[60] These are not the only events over the last several years of similar Russian activities. The harassment appears banal outside of the associated fear and risk of miscalculation by the targeted aircrew or sailors. However, in the event that tensions escalate, NATO and US forces in Europe and the Middle East are also slowly being conditioned with seemingly benign stimuli that offer little reaction time if the expected behavior changes.

Referring back to RAND's C4ISR system, conditioning via persistent unsafe Russian manevuers shapes the individual perception of operators and intelligence analysts. Further, by conducting close encounters across multiple theaters, it reinforces the perception and desired behavior for the targeted group (US and NATO forces). Importantly, it does not guarantee that the same behavior will occur at a future moment. As Skinner explains, "a response ... cannot be predicted or controlled. We can only predict that similar responses will occur in the future."[61] The probability that inaction by the pilot or sailor will occur increases with each reinforcing close encounter. However, conditioning does not guarantee that the stimulus will elicit the same response at the desired decisive momment.

Let's also evaluate Russia's narrative using Singer and Brooking's key elements. The close encounters are physical actions but support a consistent narrative: *foreign forces operating without permisison in the vicinity of Russian interests will be placed into a high risk situation by skilled pilots and sailors.* The narrative resonates with President Putin's strategic narrative of a resurgent Novorossiya. Further, it evokes outrage within the US that gains attention. The lack of a tactical response by the US gives the appearance of a strong Russian military. Finally, it subverts the narrative that the US is untouchable by demonstrating the Russian military's aptitude. In summary, close encounters are successful because they complement the strategic narrative of the Putin administration, while staying below the threshold of conflict. Further, the conditioning is tactically effective, since it elicits the desired behavior while in-

creasing the probability that the behavior will occur at a decisive moment. In short, the events are strategic and tactical victories for Russian messsage-centric warfare within the psychological domain.

Recommendations

All is not lost. Yes, the US built a force based on the "war it wanted to fight."[62] However, there is opportunity to take two evolutionary and, potentially, one disruptive step to better posture the force for Great Power Competition. First, planners should invert the relationship between the JFC's narrative and mission statement and adjust its operational objectives around that construct. Second, the JFC and his or her Joint Forces Air Component Commander (JFACC) should reallocate some analytic effort away from Warden-esque Target Systems Analysis (TSA) to relevant actor analysis and tailored message development. Finally, and most disruptively, the DOD should consider reshaping the American intelligence orientation away from secrecy and senior leaders toward transparency and the public interest.

The joint planning process has not fully internalized changes to the conflict continuum and remains focused on phases. Termination criteria remain the first requirement identified within operational design that "must be met before military operations can be concluded."[63] The idea that military operations conclude is a fallacy. Later, in reference to the Commander's Refined Planning Guidance, planners' are authorized to operate without termination criteria but may have transitions instead.[64] Transition criteria likely works better for maneuvering across the continuum of conflict. However, joint doctrine remains focused on the idea of culmination. In the chapter on operational art and design, in the section on phasing, transitions are referred to as a linear concept that ultimately ends in the "[restoration of] the conditions necessary for long-term stability."[65] There is no mention of a transition from conflict to competition or cooperation, let alone specifics related to transitioning to the associate military activities.

Much of JP 5-0, *Joint Planning,* is framed in establishing and completing tasks that result in the culmination of conflict and implicitly military activities post-conflict. This is clear within the planning guidance for the mission statement: "The joint force's mission is the task or set of tasks, together with the purposes, that clearly indicates the action to be taken and the reason for doing so."[66] To be clear, it is important to retain this approach in the event of crisis action planning. However, in Great Power Competition, where the message reigns supreme, it is more important to develop a strategic narrative that employs Singer and Brooking's key elements. Consider the example of a mission statement in JP 5-0:

> When directed, United States X Command, in concert with coalition partners, deters Country Y from coercing its neighbors and proliferating weapons of mass destruction in order to maintain security in the region.[67]

The example mission statement, when evaluated as a narrative, is simple, coherent, and relatively consistent, especially in relation to national strategy and international laws and norms. However, it lacks emotive language, does not consider the shared cultural history of the coalition partners, and does not emphasize why the community matters. It lacks the ability to gain attention with its banal language. In short, the mission statement lacks the efficacy to be successful as strategic narrative. However, the critical takeaway is not that mission statements are flawed narratives and should be rewritten as strategic narratives. Mission statements and strategic narratives are different and should be evaluated accordingly. However, a strategic narrative is more important during Great Power Competition. Therefore, any mission statements should be subsequently written to support the message. Today, the Joint Force plans in the opposite direction.

If the US military is to become message-centric and begin with a strategic narrative, it must consider new operational or tactical objectives to complement its existing toolkit within JP 3-0. In *Hostile Social Manipulation,* RAND studied the tactics and techniques employed by agents in social media and identified a set of nine common objectives. Figure 9 reframes RAND's objectives in the JFC's context:

Potential JFC Objectives

- "Improve attitudes toward" US and coalition forces
- "Generate conflict and tension among components of target" military components
- "Intimidate, silence, or render ineffective groups or individuals in" military "who are opposed to the goals" of US and coalition forces
- "Distract attention, cause confusion"
- "Discredit, destabilize, undermine or promote specific groups, institutions important to competitive strength of target country"
- "Discredit specific … leaders [or appointed commanders]" of target country opposed to US and coalition forces
- Expose illicit or illegitimate activities of governmental or military organizations
- Reinforce the truth in global societies
- Spark desired behavior among highly targeted populations or groups (voting, protest)

Figure 9. Derived from RAND's objectives of social manipulation campaigns.[68]

In order to operate in support of the above objectives, some portion of the intelligence enterprise must reorient towards relevant actor analysis and tailored-message development. Referring back to then-General Mattis' argument against EBO: "It assumes a level of unachievable predictability [and] ... is too prescriptive and overengineered [by discounting] the human dimensions of war (for example, passion, imagination, willpower, and unpredictability)."[69] Con-

versely, General Mattis acknowledged the need to retain the ability to "[create] unity of action in employing nodal analysis as it relates to targeting."[70] In short, do not force the same process on all scenarios. So, while the Warden approach to analysis against target systems like IADS must be retained, the Joint Force must consider complex systems like relevant actors.

If the primary weapon in message-centric warfare is the narrative, then intelligence analysts must partner with cultural subject matter experts, behavioral scientists, and public affairs specialists to understand the way the group's attention will be earned, how the message will be received, and how it may or may not reinforce the desired behavior. Relevant actor analysis should consider trust relationships between individuals and within groups. How often do individuals communicate within the system? What are the means of communication? As early as 1995, George Stein recognized the value of emergent mass media technologies. He argued, "A major new factor in information war is the worldwide infosphere of television and broadcast news."[71] Today, a majority of person-to-person engagements, whether financial or social, occur through Weibo in China. Culturally, what are the relevant actor's norms? In order to expose a leader's illicit or illegitimate activities, it is critical to understand the way the community perceives those activities in the first place.

These and other questions must be answered by a team performing relevant actor analysis prior to considering any capabilities to achieve the operational objective. Analysts must also approach the Joint Integrated Prioritized Target List inversely to the current model. Even in large-scale combat, due to the long lead-time to develop tailored messages, computer exploits, or waveforms, these capabilities should be considered prior to kinetic capabilities. However, in the case of competition, the tailored message for prioritized relevant actors should be considered before any potential actions are planned.

Once the analysis is complete, electronic warfare, information operations, or cyberspace operations offer potential means to shape the information environment favorably for the intended strategic narrative. Again, as Stein argued, "Information warfare at the strategic level is the 'battle off the battlefield' to shape the political context of the conflict."[72] This remains the case across the continuum of conflict today. To support the JFC's strategic narrative, personnel must orient towards these relevant actors in coordination with Defense Attaché Offices to develop an operational design that ultimately supports the JFC's message.

Finally, to truly approach the authenticity required for a strong strategic narrative, it is time for the DOD to consider an alternative approach to intelligence: one that focuses on transparency and public interest over secrecy and senior leaders. In late January 2020, General John Hyten, Vice Chairman of the Joint Chiefs of Staff, blasted the execution of the classification process within the Pentagon, lamenting rampant over-classification to the point of organizational harm.[73] In Decem-

ber 2019, Air Force Secretary Barbara Barrett testified to Congress regarding space programs that "You would have to be careful about what we declassify, but there is much more classified than what needs to be"; Representative Mike Rogers concurred.[74] Representative Rogers, Secretary Barrett, and General Hyten are leading in the right direction.

Intelligence classifications are predicated on protecting the sources and methods by which the information was gathered. To be clear, the US should not breach this contract with the intelligence community. Rather, a comparative study should be done to evaluate whether the general public can reasonably assume the technical means by which collection operations are executed. For example, if a private company possesses the capacity to provide an information-gathering service to the public, then it can be reasonably assumed that the government possesses similar capability or technical means. When the appropriate threshold is met and the information can be declassified, the DOD should take the next step and provide an open source repository for trusted media outlets. By focusing on declassifying as many sources of information as possible while not detracting from national security, the US government can employ transparency as a means to increase its authenticity while placing the general public closer to the ground truth.

To support the public further, the Joint Force can reorient many of its analysts towards a Bellingcat-style reporting, leveraging publicly available information. Bellingcat first burst onto the scene in mid-2014 with its detailed analysis of public information, characterizing the downing of Malaysian Airlines Flight 17 by the Russian government. As Russia sought to deny the accusations, the Bellingcat team published report after report that ultimately exposed the truth.[75] Amid tit-for-tat exchanges between the Russian and US government that failed to come to a conclusion, the open source investigative team provided an alternative independent analysis backed by multiple sources for public consumption. The strategic narrative battle is not between senior leaders, but rather between multiple relevant actors with different cultural histories. Increasing transparency and focusing on delivering the truth to the public in coordination with like-minded liberal democracies would enhance the JFCs' strategic narratives by increasing authenticity and discrediting our competitors by exposing their illicit gray zone tactics.

Conclusion

The United States does not currently possess the force or processes to fight in the psychological domain and deal with the primary tactics of its competitors in Great Power Competition. The American legacy strategy under a unipolar world to maintain the status quo as the global hegemon is untenable. Great Power Competition has three key characteristics: (1) the emergence of alternatives to the current world order creates a geopolitical marketplace for rational actors' choice; (2) the comparative na-

tional power between Great Powers increases the global and national risk of large scale combat beyond the willingness of decision-makers to transition from competition to conflict; and (3) the preceding factors necessitate the employment of gray zone tactics for competitors to achieve national policy objectives without risking conflict.

The Joint Force must modify its operational approach in accordance with these characteristics. Great Powers studied the United States' way of war and developed a strategy and tactics that avoid US strengths and exploit its vulnerabilities. As a result, US operations across the continuum of conflict, specifically military engagement, security cooperation, deterrence, crisis response, and limited contingency operations must shift from a systems-centric approach that is effective on closed-systems like an Integrated Air Defense System. Instead, the Joint Force should adopt a message-centric approach. The strategic narrative should drive all subsequent actions and adhere to Singer's and Brooking's principles of social media warfare: *narrative, emotion, authenticity, community,* and *inundation.* At the tactical level, commanders should be cognizant of physical actions that simultaneously support a strategic narrative but prepare the psychological domain for operations. For example, conditioning operations to shape the desired behavior prior to conflict.

The Joint Force can take two evolutionary and, potentially, one disruptive step toward Great Power Competition. First, it can adjust its current planning process by constructing a strategic narrative and designing the mission statement and its associated objectives to support the message. Among those objectives, joint planners should consider some identified by the RAND Corporation in its *Hostile Social Manipulation* study. Joint force narratives should be tailored for relevant actors. As a result, the Joint Force Commander requires personnel dedicated to relevant actor analysis and tailored message development. Finally, the Joint Force should critically evaluate its current intelligence sources and methods to determine what can be declassified to ultimately increase the amount of publicly available information to trusted media sources. By combining open source analysis of publicly available information supported by newly declassified sources and methods, the US would be better positioned to shape the global narrative via authenticity and transparency to counter the illicit gray zone warfare employed by its competitors.

Jeremiah Deibler holds a MA in Diplomacy from Norwich University and is currently completing his MA in Military Operational Art and Science at Air University within the Multidomain Operational Strategist concentration. He is an Intelligence Officer in the United States Air Force. Over his 11 years of service, Jeremiah developed

experience in national and theater ISR operations in support of ground, air, space, and cyberspace operations to include a deployment to Afghanistan and Qatar. After completing the Intelligence Weapons Instructor Course in June 2016, he served as the Chief of Weapons and Tactics for ISR for and from Cyberspace. Upon graduation from Air Command and Staff College in June 2020, Jeremiah will be assigned to the 460th Space Wing as the Senior Intelligence Officer.

Jeremiah.Deibler@gmail.com

Notes

1 Lily Kuo, "'American Coronavirus': China Pushes Propaganda Casting Doubt on Virus Origin," The Guardian, March 12, 2020, https://www.theguardian.com/world/2020/mar/12/conspiracy-theory-that-coronavirus-originated-in-us-gaining-traction-in-china.

2 Ibid.

3 @zlj517. March 12, 2020. "CDC was caught on the spot. When did patient zero begin in US? How many people are infected? What are the names of the hospitals? It might be US army who brought the epidemic to Wuhan. Be transparent! Make public your data! US owe us an explanation!" [Twitter post]. https://twitter.com/zlj517/status/1238111898828066823?s=20.

4 @jabinbotsford. March 19, 2020." Close up of @realDonaldTrump notes is seen where he crossed out "Corona" and replaced it with "Chinese" Virus as he speaks with his coronavirus task force today at the White House. #trump #trumpnotes." [Twitter post]. https://twitter.com/jabinbotsford/status/1240701140141879298?s=20.

5 Ibid.

6 Joint Publication 3-0, Joint Operations, October 22, 2018, VI-6.

7 Francis Fukuyama, "The End of History?" The National Interest 16 (Summer 1989): 3.

8 Louis Menand, "Francis Fukuyama Postpones The End of History", The New Yorker, August 27, 2018, https://www.newyorker.com/magazine/2018/09/03/francis-fukuyama-postpones-the-end-of-history.

9 Elena Moore, "Timeline: How the U.S. Came To Strike And Kill A Top Iranian General," National Public Radio, January 4, 2020, https://www.npr.org/2020/01/04/793364307/timeline-how-the-u-s-came-to-strike-and-kill-a-top-iranian-general.

10 Alan Yuhas and Raya Jalabi, "Ukraine Crisis: Why Russia Sees Crimea as its Naval

Stronghold," The Guardian, March 7, 2014, https://www.theguardian.com/world/2014/mar/07/ukraine-russia-crimea-naval-base-tatars-explainer.

11 Andrew Chatzky and James McBride, "China's Massive Belt and Road Initiative," Council on Foreign Relations, January 28, 2020, https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative.

12 Office of the Secretary of Defense, National Defense Strategy of the United States of America (2018), 2.

13 Andreo Calonzo, "Duterte Wants Stronger Defense Ties with Russia, Criticizes US," Bloomberg News, October 4, 2019, https://www.bloomberg.com/news/articles/2019-10-04/duterte-wants-stronger-defense-ties-with-russia-criticizes-u-s.

14 Xi Jinping, The Governance of China II (Beijing: Foreign Language Press, 2017), 42.

15 Ibid.

16 Philip Citowicki, "China's Reach Tests the Pacific's Fragile Island Democracies," Foreign Policy, January 7, 2020, https://foreignpolicy.com/2020/01/07/chinas-reach-tests-the-pacifics-fragile-island-democracies/.

17 Tom Hanson, "Australia and China: A View from the US," Australian Strategic Policy Institute: The Strategist, October 28, 2019, https://www.aspistrategist.org.au/australia-and-china-a-view-from-the-us/.

18 Amanda Donnelly, "Finding a Method for the Madness: A Comparative Analysis of Strategic Design Methodologies," School of Advanced Air and Space Studies, Air University, June 2017, 58–60, https://pdfs.semanticscholar.org/d482/99e559b8cded6615a68958f639e4e7441f10.pdf.

19 Office of the Secretary of Defense, National Defense Strategy.

20 United States House of Representatives, "Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements," Permanent Select Committee on Intelligence, https://intelligence.house.gov/social-media-content/.

21 Vince Beiser, "Aboard the Giant Sand-Sucking Ships that China Uses to Reshape The World," MIT Technology Review, December 19, 2018, https://www.technologyreview.com/s/612597/aboard-the-giant-sand-sucking-ships-that-china-uses-to-reshape-the-world/.

22 Center for Strategic and International Studies, "Still Under Pressure: Manila Versus The Militia," Asia Maritime Transparency Initiative, April 16, 2019, https://amti.csis.org/still-under-pressure-manila-versus-the-militia/.

23 Beiser, "Aboard the Giant Sand-Sucking Ships."

24 Christopher Andrew and Vasili Mitrohkin, The World was Going our Way: The KGB and the Battle for the Third World (New York: Basic Books, 2005), 1.

25 The Wilson Center, "Timeline: the Rise, Spread, and Fall of the Islamic State," October 28, 2019, https://www.wilsoncenter.org/article/timeline-the-rise-spread-and-fall-the-islamic-state.

26 The White House, "National Security Council," March 2, 2020, https://www.whitehouse.gov/nsc/.

27 Office of the President of the United States, National Security Strategy of the United States of America, December 2017, 33.

28 Ibid., 34.

29 Ibid.

30 James Mattis and Joseph Dunford, "Briefing by Secretary Mattis on US Strikes in Syria," United States Department of Defense, April 13, 2018.

31 James N. Mattis, "USJFCOM: Commander's Guidance for Effects-Based Operations," Joint Forces Quarterly 51 (4th Quarter 2008): 105.

32 Ibid., 106.

33 Michael R. Gordon and General Bernard E. Trainor, The General's War (New York: Little, Brown and Company: Hachette Book Group, 1995), 107.

34 Chris Morris, Janet Morris, and Thomas Baines, "Weapons of Mass Protection: Nonlethality, Information Warfare, and Airpower in the Age of Chaos," Airpower Journal (Spring 1995): 24.

35 George H.W. Bush, National Security Directive 54, January 15, 1991.

36 George H.W. Bush, Address on Iraq's Invasion of Kuwait – Operation Desert Shield, August 8, 1990, https://www.americanrhetoric.com/speeches/georgehwbushkuwaitinvasion.htm.

37 Leaflets of the Persian Gulf War (Fort Bragg, NC: 4th Psychological Operations Group [Airborne], 1991), https://www.psywar.org/psywar/reproductions/LeafletsPersianGulfWar.pdf, 2.

38 Ibid.

39 Qiao Liang and Wang Xiangsui, Unrestricted Warfare (Beijing: PLA Literature and Arts Publishing House, 1999), 11–12.

40 Ben Connable, Jason H. Campbell, and Dan Madden, "Stretching and Exploiting Thresholds for High-Order War," RAND Corporation (2016), https://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1003/RAND_RR1003.pdf, 7.

41 Qiao and Wang, Unrestricted Warfare, 20.

42 Ibid., 33.

43 Ibid., 25.

44 Mark Powerleau, "Here's How Other Nations Measure up in Electronic Warfare," C4ISRNet, March 14, 2019, https://www.c4isrnet.com/electronic-warfare/2019/03/14/heres-how-other-nations-measure-up-in-electronic-warfare/.

45 Sebastien Roblin, "A2/AD: The Phrase that Terrifies the U.S. Military (And China and Russia Love It)," The National Interest, April 9, 2019, https://nationalinterest.org/blog/buzz/a2ad-phrase-terrifies-us-military-and-china-and-russia-love-it-51597.

46 Justin Sherman, "Russia and Iran Plan to Fundamentally Isolate the Internet," Wired, June 6, 2019, https://www.wired.com/story/russia-and-iran-plan-to-fundamentally-isolate-the-internet/.

47 Jeremiah Deibler, "Winning Wars of Cognition: Posturing the Air Force for the Tactical Information Fight," Over the Horizon Journal, February 10, 2020, https://othjournal.com/2020/02/10/winning-wars-of-cognition-posturing-the-air-force-for-the-tactical-information-fight/.

48 Ibid.

49 Walter Perry, David Signori, and John Boon, "Exploring Information Superiority: A Methodology for Measuring the Quality of information and Its Impact on Shared Awareness," RAND Corporation (2004), 10, https://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR1467.pdf.

50 Ibid.

51 Stanislas Dehaene, Consciousness and the Brain: Deciphering How the Brain Codes our Thoughts (New York: Penguin Books, 2014), 141–75.

52 Peter Singer and Emerson Brooking, LikeWar: The Weaponization of Social Media (New York: Houghton Mifflin Harcourt Publishing Company, 2019), 154.

53 Ibid, 154–80.

54 B.F. Skinner, Science and Behavior (New York: The Free Press, 1953), 47.

55 Ibid, 53.

56 Ibid, 77–78.

57 Ibid, 82–83.

58 "Russia Intercepts U.S. Spy Plane in 'Dangerous' Maneuver Off Syrian Coast," Haaretz, June 6, 2019,https://www.haaretz.com/middle-east-news/russia-intercepts-u-s-spy-plane-in-dangerous-maneuver-off-syria-coast-1.7333886.

59 Commander 7th Fleet Public Affairs, "Russian Navy Ship Maneuvers Unsafe, Unprofessional," US 7th Fleet, June 7, 2019, https://www.c7f.navy.mil/Media/News/Display/Article/1869114/russian-navy-ship-maneuvers-unsafe-unprofessional/.

60 Ryan Browne, "NATO Accuses Russian Jet of Conducting 'Unsafe' Maneuver During

Aerial Encounter," CNN, August 15, 2019, https://www.cnn.com/2019/08/14/politics/nato-russia-jets-unsafe/index.html."

61 BF Skinner, Science and Behavior, 64-65.

62 Qiao and Wang, 33.

63 Joint Publication 5-0, Joint Operations, June 16, 2017, IV-19.

64 Ibid., V-19.

65 Ibid., IV-41–IV-42.

66 Ibid., V-4.

67 Ibid., V-4.

68 Michael J. Mazarr et al., "Hostile Social Manipulation: Present Realities and Emerging Trends," RAND Corporation (2019), 19, https://www.rand.org/pubs/research_reports/RR2713.html.

69 Mattis, "USJFCOM," 106.

70 Ibid., 107.

71 George Stein, "Information Warfare," Airpower Journal (Spring 1995): 33.

72 Ibid.

73 Aaron Mehta, "The Military's 2nd-Highest-Ranking Officer Wants to Change the Pentagon's 'Unbelievably Ridiculous' Classification Process," Business Insider, January 30, 2020, https://www.businessinsider.com/hyten-wants-to-change-unbelievably-ridiculous-pentagon-classification-2020-1.

74 Nathan Strout, "Barrett, Rogers Consider Declassifying Secretive Space Programs," DefenseNews, December 7, 2019, https://www.defensenews.com/smr/reagan-defense-forum/2019/12/08/barrett-rogers-plan-to-declassify-black-space-programs/.

75 Bellingcat Investigative Team, "Posts Tagged: MH17," Bellingcat, March 26, 2020, https://www.bellingcat.com/tag/mh17/.

Review of *LikeWar: The Weaponization of Social Media*

P. W. Singer and Emerson T. Brooking. *LikeWar: The Weaponization of Social Media.* Boston: Mariner Books, Houghton Mifflin Harcourt, 2019. ISBN: 978-0-35-810047-4 (Pbk). 273 pages. $15.99

"Social media." It needs no introduction: we are obsessed with it. Facebook vacation albums, glossy Instagram images, live concerts on Snapchat, on-demand YouTube entertainment—this is our new digital reality. Social media has revolutionized our information spaces aimed at connecting the world's people through our daily experiences. Most of us, however, know that it often fails to *truly* connect us. Instead, this digital frontier has fallen prey to grabs for virtual influence, brand-building, confrontations, and the viral spread of information—benign and otherwise. Because of its massive reach, social media has even become an effective instrument for nation states, and everyone between, to behave much the same. *LikeWar,* addressing this sobering reality, is as timely as it is good. Presenting a research-filled warning to the American public, Singer and Brooking present the new normal of our digital lives. Using diverse examples ranging from Taylor Swift to ISIS and Donald Trump to the Arab Spring, *LikeWar* explains how the internet, and particularly social media, evolved from a creative way of connecting people to a means of attacking them.

Several observations come from the authors' study of this new digital environment. First, Singer and Brookings detail how the internet, beginning from the basements of US universities, enabled social media's emergence. The internet alone connects hundreds of millions of people—and will eventually include most of the world's population. Information used to travel as far as the courier could run, the paperboy could pedal, the length of telegraph cable laid, and the miles the radio waves traveled. Today, the internet shotguns information across continents in milliseconds, with few and decreasing limitations. Although its development has been rapid, the internet has stabilized, and will likely continue as a cornerstone of human life for the foreseeable future.

Secondly, *LikeWar* notes that social media is not the beacon of hope its developers designed it to be. Rather, social media is a battlefield. This battlefield does not have fields and bullets, however. It has chat rooms (and hashtags, and pages, and forums!) and messages—and just as importantly, winners and losers. Singer and Brooking explain that the internet is "a platform for achieving the goals of whichever actor manipulates it most effectively" (261). Victories won on this battlefield are not limited to eliminating your target. Conversely, belligerents want to control their enemies through attention, engagement, and allegiance.

 doi: 10.18278/gsis.5.1.10

Lastly, this virtual battlefield has erupted across all routines of modern society—combatants and civilians alike are caught in this messaging crossfire. Often happening beneath the surface, many are unaware they're a part of the fight. These new battles puree the categories of war and politics so well they've become indistinguishable. Clausewitz claimed war was just an extension of politics; *LikeWar* sees them as the same thing altogether. In *LikeWar,* there is hardly room for categorical claims of "war" and "peace" because the war is already happening—it just looks different.

LikeWar details the realities of these new battlefields through narrative—stories to pull the reader into the details of social media's contribution to historical events. Each chapter begins with a story: from Donald Trump's resurrected political career with help from Twitter; the ability of ISIS, with marginal numbers, to incite panic and surrender from an entire nation through a massive (and fictitious) digital army; the internet's beginnings in the basement of a musty UCLA basement; Mark Zuckerberg's Harvard dorm room startup now known as Facebook; and the Russian government's covert, virtual invasion of American political dialogues to sow chaos and division.

For many, *LikeWar* will be an informative reset—or introduction—to the realities of social media. This book is for everyone that has a social media account or knows someone who does. *LikeWar* is for everyone. Singer and Brooking created a special book that blends the feel of pop psychology with the research depth demanded from a peer-reviewed journal. For this, the authors deserve praise for appealing to many audiences without losing the importance and depth of their message. It would be remiss, however, to assume the authors did not have particular audiences in mind when writing the book. At the book's conclusion, *LikeWar* makes recommendations for navigating the new digital normal for two primary audiences: social media executives and lawmakers. The message? To executives—accept the political and social power your platforms have given you as arbiters of truth. To governments—take the emerging battlefields seriously; this is not an issue just for youth.

LikeWar has much more to praise than critique. Yet there is room for improvement, namely in the book's proposed solutions to the issues we face. In fairness, the aim of the work was not to offer a "fix" for problems, but its recommendations were imprecise and even weak. Given the exhaustive research on the topic, there are few like Springer and Brooking available to offer credible insight to leaders across government and industry. However, *LikeWar* hesitates to explicitly offer policy suggestions. There are some, like information literacy programs for our youth, but many suggestions fall short of actions we can take today. The policy-changing potential of the book is already strong; it would have been more so with sharper, direct policy considerations.

Nevertheless, the positives far outweigh the few areas of improvement. *LikeWar* spends nearly a third of its weight in bibliography. In a world given to sensationalism, the diligence required to produce a work of this merit is refreshing and gives the reader confidence in its message. Better yet, the research is engaging and sustains the reader to the end. Many texts cover a subject in great detail but fall short in telling a story as captivating as *LikeWar*.

In summary, *LikeWar* analyzes and comments on arguably the most important global security threat of our day: the internet, social media, and their weaponization. Singer and Brooking leave behind a punch to the jawlines of Americans and world citizens alike, operating under the ignorant assumption that their online worlds are safe. People—nations—are fighting. The solution? I am not sure anyone knows. But in the meantime, let's take a lesson from social media and "share" this book with our friends.

Austin Gouldsmith

Review of *Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News*

Clint Watts (2019). *Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News*. New York: HarperCollins. ISBN: 978-0-06-279599-1 (Hbk), 978-0-06-295649-1 (Ebk). 314 pages. $16.99 (Hbk)

Is social media helpful or harmful? Clint Watts explores the role of social media and an interconnected world in enabling and preventing terrorism and propaganda. Watts does not shy away from sharing his personal experiences with the reader, which makes "Messing with the Enemy" accessible to a wide audience from laypeople hoping to understand the effects of Russian troll farms to intelligence and influence operations professionals seeking a summary of past and recent events. Combining professional expertise with a thoroughly researched topic leads to a very readable and informative account of how psychological warfare has evolved in a social media world.

Social media allows people from all over the world to connect, to share their thoughts, and it is now a main news source for people throughout the world. While this interconnectedness has its benefits, Watts highlights how social media is used to manipulate people's beliefs and actions. He describes how Islamic extremist organizations have been using social media to "radicalize, recruit, operate, finance, train, and direct" through websites like Facebook, Twitter, and Youtube since these sites first emerged. Social media boosted al-Qaeda's recruiting, a Jihadi blog called *Inspire* called for violence across the world, and al-Shabaab utilized Twitter to mobilize a younger audience. While the U.S. intelligence community once had the advantage in understanding extremist Islamic groups, social media rapidly allowed anyone to gain insight into how terrorists thought and communicated.

Watts also discusses Russia's utilization of social media to influence people through an exploration of Russia's history beginning with traditional media to the rise of the Kremlin's social media use. Russian troll farms, with quotas on social media posts and comments, certainly played an unwanted role in the 2016 election. Hacking was used to get information, which was then strategically leaked in order to achieve specific effects. The author does not claim to know the extent of the effects of Russia's meddling had on the United States, but, like Robert Mueller's July 2019 testimony, warns of Russia's previous and continued meddling in U.S. elections and politics.

 doi: 10.18278/gsis.5.1.11

Messing with the Enemy focuses primarily on how people came to rely on social media as a source of information and how this has backfired when people believe, repeat, and act on propaganda. While the majority of the book details the history of influence through social media, the true meat of the book comes in the last few chapters, with Watts's discussion on why messaging is so effective, the future of influence, and his advice on surviving in a social media world.

War is constantly changing, and the war of ideas is facilitated through social media. The author addresses some of the reasons the United States cannot compete with Russia's efforts in influence operations—heavy-handed oversight, a lack of ownership of the messages, and a betrayal of U.S. ideals. Influence operations cannot be used on an American audience, but this line blurs with such open access to social media. How do we determine who the potential audience of a message is? Watts contends that the U.S. government has not been able to determine who has responsibility for messaging, so no entity has responsibility over counter propaganda. Within the military, influence operations tends to be split between public affairs, information operations, and psychological operations (PSYOP). If the United States used the same tactics as Russia, our American values would be eroded. Without upholding those values, the U.S. would lose credibility on the world stage.

While Watts acknowledges that he may sound pessimistic, he attempts to propose a way forward. One suggestion involves placing more responsibility on social media sites to vet news, perhaps in the form of "Information Consumer Reports". Unfortunately, while Facebook News claims to be vetting news sources in the way Watts envisioned, the site immediately faced criticism for including sites like Breitbart as trusted news sources. For corporations, he recommends protecting against propaganda just as thoroughly as they protect against hacking. For the individual, Watts has a few suggestions for self-inoculation towards susceptibility to fake news. Instead of blocking trolls or people who disagree, expose yourself to how others think. Try to understand why they think the way they do, and ask under what conditions an idea would be wrong. Analyze sources through determining their competency, motivation, product, and process. Lastly, reduce social media time. This last suggestion should not come as a surprise – study after study shows how an excess of social media time leads to people being less satisfied, less connected, and, as Watts proclaims, less informed.

Overall, *Messing with the Enemy* blends Clint Watts' personal experience in social media influence operations against terrorist organizations with analysis of the history, tactics, and successes of adversaries like Russia or extremist organizations. This discussion is rounded out with his perspective on the current U.S. and global situation as well as his thoughts and predictions for the future. The primary shortcoming of this book was the lack of detailed analysis into the psychology of why some types of fake news are so successful while others lag behind. Howev-

er, the final chapters on "surviving in a social media world of hackers, terrorists, Russians, and fake news" are pithy, thought provoking, and not to be missed. As asymmetric conflict moves swiftly into the information theater, Watts's writing on the subject is timely and informative.

Sarah Soffer

Review of *The Conduct of Intelligence in Democracies: Processes, Practices and Cultural*

Florina Cristiana Matei and Carolyn Halladay, eds. *The Conduct of Intelligence in Democracies: Processes, Practices and Cultural.* London: Routledge Lynne Reinner Publishers, 2019. ISBN: 9781626378216. 278 pages. $45.00 (hardcover)

In *The Conduct of Intelligence in Democracies: Processes, Practices and Cultural,* editors Florina Cristiana Matei and Carolyn Halladay fill a gap in intelligence literature, that of a comparative study between international intelligence practices. In their words, they seek "to provide readers with international views on the role and place of (effective) intelligence in a democratic milieu" (xi). There are of course challenges in achieving such an objective when the subject matter they are investigating is by its very nature composed of classified information and secret operations. The authors offer a wide range of case studies from various regions including Africa, Asia, Eastern Europe, and Latin America.

Both seasoned intelligence professionals and early stage academics alike will find this text a compelling study of intelligence work in democratic society. The forward is written by University of Leicester Head of Director of Politics and International Relations Professor Mark Phythian. In noting the timely relevance of this text, he explains that "intelligence has to be about more than improving professional practice ... because [conducting intelligence] raises fundamental questions about the relationships between state and citizen, openness and secrecy, accountability and deniability, inward and outward focus, and the legitimate aims and limits of intelligence in a democratic context" (vii).

The authors provide in-depth analyses of the relationship between democratically elected leaders and agency operations, the role of intelligence led policing, the psychological relationships among political, geographical, and agency culture, and the effect that culture has on achieving intelligence objectives. Of particular interest to this issue of *Global Security and Intelligence Studies*, and a strength in this compilation of insightful essays, is the authors' application of psychological theory to themes threaded throughout this comparative study of intelligence.

For example, in Chapter 1, the editors lay a firm foundation upon which the rest of book is built; of interest here, they list three challenges to the intelligence processes in democracies: 1) external actors that may threaten national security, 2) internal policy constraints that prevent cooperation between agencies, and 3) inherent human psychological limitations. The authors emphasize a simple but often overlooked human factor: the role of cognitive and deductive ability. They

 doi: 10.18278/gsis.5.1.12

list polarized objectives that can frustrate judgment calls. Some of these include "intelligence priorities (averting crime versus fighting terrorism), interests (objectivity versus policy influence and persuasion), and needs (the need to know versus the need to share, centralization versus decentralization of agencies)" (8).

The authors explain that the degree of weight given to either end of these dichotomous objectives is determined by the culture of the agency's parent political psychology. Since the goal of much international intelligence is to movie nations towards a status of *consolidated democracy*, even after conversion, the past legacy of former intelligence structures cannot be ignored. Typically, two paths are taken: the new intelligence agency is built directly upon the old (as in Czechia, Poland, Uruguay, etc.) or there is a splitting of new and old agencies (as in Romania, Argentina, South Korea, etc.). In either case, residual practices can "perpetrate mistrust" and even create what Frank Church, for whom the Church Committee was named (later called the Senate Select Committee on Intelligence), called "rogue elephants" (15).

Chapter 14 is written by Irena Chiru of the National Security Academy and is titled "National Security Cultures." It starts with a quote by Colin S. Gray, Professor of International Relations and Strategic Studies at University of Reading: "All strategic behavior is affected by humans who cannot help but be cultural agents" (213). The national-political culture and the agency-specific culture can directly impact our capabilities. Expanding on Gray's observation, Chiru explains that "cultural variables are perceived as significant factors in understanding, explaining, and predicting the way intelligence is organized, performed, and perceived [and help in] explaining the role and impact of myths, symbols, social norms, history, nature of organizations, narrative, perceptions, and the (political) psychology of social actors" (213).

Chiru calls intelligence culture "strategic culture" and claims that in engaging in a degree of self-reflection, intelligence failures can be better understood and managed. Joanisval Brito Gonçalves, Federal Consultant and Professor on International Affairs in Brazil, in his chapter titled "Counterintelligence," echoes the importance of understanding the connection between intelligence culture and operation failure when it triggers counterintelligence investigations. Gonçalves uses the example of Brazil, and discusses how intelligence failures can be caused by criminal organizations that infiltrate law enforcement, corrupting its culture.

As noted above, Chiru focuses on the impact of myths and social norms both on internal and external processes. She explains that after the retraction of communism, and to a degree its governing and intelligence infrastructure, there was vacuum that needed to be filled. This vacuum was filled with both pre-Soviet cultural ideologies but also with what came to be known as the "western savior" concept. Romania faced an almost complete reform of both "political and social structures" (221). There had to be a shift in the social perception of the security

sector and this was effectively done using language, by implementing a new vocabulary in the culture, according to Chiru. This book is filled with similarly instructive examples offered by well-informed contributors.

Content-wise, in the end there is an intelligence-and-democratic dilemma that grows from the need for secrecy in intelligence work and for transparency and accountability in democratic systems. Intelligence agencies must function as small bureaucratic entities within the larger democratic bureaucratic system. The authors in this book do right in highlighting the critical importance of finding a balance in communication with politicians that is transparent to the extent that sensitive information is protected.

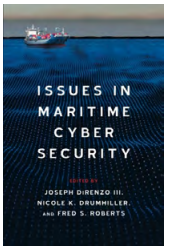
As the editors write, "The function of intelligence involves two processes that may be separate or intertwined: inductively solving a puzzle, understood as a mosaic, the shape of which is by and large known and which could be solved with certainty through accessing a specific type of data or information" (5). In order for information to be used strategically as intelligence, it needs to be controlled. Doing this while retaining public trust is the democratic ideal.

Joel Wickwire

This publication is available open access at:
http://www.ipsonet.org/publications/open-access

Thanks to the generosity of the American Public University System

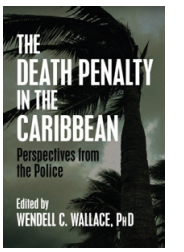
Featured Titles from Westphalia Press



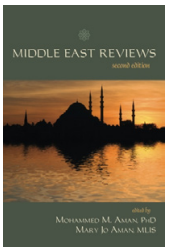
Issues in Maritime Cyber Security Edited by Nicole K. Drumhiller, Fred S. Roberts, Joseph DiRenzo III and Fred S. Roberts

While there is literature about the maritime transportation system, and about cyber security, to date there is very little literature on this converging area. This pioneering book is beneficial to a variety of audiences looking at risk analysis, national security, cyber threats, or maritime policy.

The Death Penalty in the Caribbean: Perspectives from the Police Edited by Wendell C. Wallace PhD



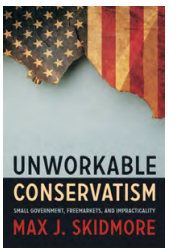
Two controversial topics, policing and the death penalty, are skillfully interwoven into one book in order to respond to this lacuna in the region. The book carries you through a disparate range of emotions, thoughts, frustrations, successes and views as espoused by police leaders throughout the Caribbean



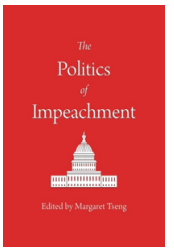
Middle East Reviews: Second Edition
Edited by Mohammed M. Aman PhD and Mary Jo Aman MLIS

The book brings together reviews of books published on the Middle East and North Africa. It is a valuable addition to Middle East literature, and will provide an informative read for experts and non-experts on the MENA countries.

Unworkable Conservatism: Small Government, Freemarkets, and Impracticality by Max J. Skidmore



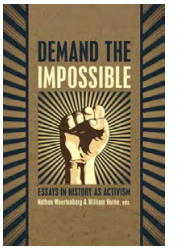
Unworkable Conservatism looks at what passes these days for "conservative" principles—small government, low taxes, minimal regulation—and demonstrates that they are not feasible under modern conditions.



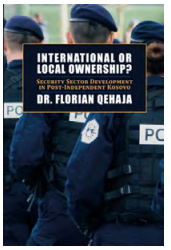
The Politics of Impeachment
Edited by Margaret Tseng

This edited volume addresses the increased political nature of impeachment. It is meant to be a wide overview of impeachment on the federal and state level, including: the politics of bringing impeachment articles forward, the politicized impeachment proceedings, the political nature of how one conducts oneself during the proceedings and the political fallout afterwards.

Demand the Impossible: Essays in History as Activism
Edited by Nathan Wuertenberg and William Horne



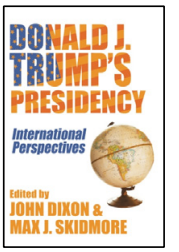
Demand the Impossible asks scholars what they can do to help solve present-day crises. The twelve essays in this volume draw inspiration from present-day activists. They examine the role of history in shaping ongoing debates over monuments, racism, clean energy, health care, poverty, and the Democratic Party.



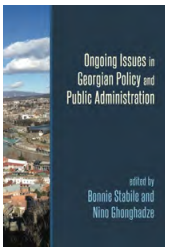
International or Local Ownership?: Security Sector Development in Post-Independent Kosovo
by Dr. Florian Qehaja

International or Local Ownership? contributes to the debate on the concept of local ownership in post-conflict settings, and discussions on international relations, peacebuilding, security and development studies.

Donald J. Trump's Presidency: International Perspectives
Edited by John Dixon and Max J. Skidmore



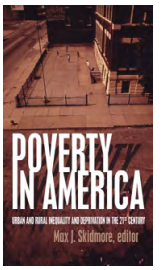
President Donald J. Trump's foreign policy rhetoric and actions become more understandable by reference to his personality traits, his worldview, and his view of the world. As such, his foreign policy emphasis was on American isolationism and economic nationalism.



Ongoing Issues in Georgian Policy and Public Administration
Edited by Bonnie Stabile and Nino Ghonghadze

Thriving democracy and representative government depend upon a well functioning civil service, rich civic life and economic success. Georgia has been considered a top performer among countries in South Eastern Europe seeking to establish themselves in the post-Soviet era.

Poverty in America: Urban and Rural Inequality and Deprivation in the 21st Century
Edited by Max J. Skidmore



Poverty in America too often goes unnoticed, and disregarded. This perhaps results from America's general level of prosperity along with a fairly widespread notion that conditions inevitably are better in the USA than elsewhere. Political rhetoric frequently enforces such an erroneous notion.