VOLUME 6 ▪ NUMBER 1 WINTER 2021

THE CYBER DEFENSE REVIEW

Fifth Generation Wireless Development in Great Power Competition: Department of Defense Implications and Policy Recommendations
Brig. Gen. Darrin Leleux, Capt. Robert Woodruff
Col. Kristy Perry, Cmdr. David Bergesen

ARMY CYBER INSTITUTE ◆ WEST POINT

The Cyber Defense Review

Winter Edition

THE CYBER DEFENSE REVIEW

A DYNAMIC MULTIDISCIPLINARY DIALOGUE

DIRECTOR, ARMY CYBER INSTITUTE
Col. Jeffrey M. Erickson

CHIEF OF STAFF, ARMY CYBER INSTITUTE
Col. Stephen S. Hamilton

SENIOR FACULTY MEMBER, ARMY CYBER INSTITUTE
Dr. Edward Sobiesk

EDITOR IN CHIEF
Dr. Corvin J. Connolly

MANAGING EDITOR
Dr. Jan Kallberg

ASSISTANT EDITORS
West Point Class of '70

AREA EDITORS

Dr. Harold J. Arata III
(Cybersecurity Strategy)

Lt. Col. Todd W. Arnold, Ph.D.
(Internet Networking/Capability Development)

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

Maj. Nathaniel D. Bastian, Ph.D.
(Advanced Analytics/Data Science)

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

Dr. Dawn Dunkerley Goss
(Cybersecurity Optimization/Operationalization)

Dr. David Gioe
(History/Intelligence Community)

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

Dr. Michael Grimaila
(Systems Engineering/Information Assurance)

Dr. Steve Henderson
(Data Mining/Machine Learning)

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

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

Dr. Fernando Maymi
(Cyber Curricula/Autonomous Platforms)

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

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

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

Ms. Elizabeth Oren
(Cultural Studies)

Dr. David Raymond
(Network Security)

Lt. Col Robert J. Ross, Ph.D.
(Information Warfare)

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

Dr. David Thomson
(Cryptographic Processes/Information Theory)

Dr. Robert Thomson
(Learning Algorithms/Computational Modeling)

Lt. Col. Natalie Vanatta, Ph.D.
(Threatcasting/Encryption)

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

EDITORIAL BOARD

Dr. Andrew O. Hall, (Chair.)
Marymount University

Dr. Amy Apon
Clemson University

Dr. Chris Arney
U.S. Military Academy

Dr. David Brumley
Carnegie Mellon University

Col. (Ret.) W. Michael Guillot
Air University

Dr. Martin Libicki
U.S. Naval Academy

Dr. Michele L. Malvesti
Financial Integrity Network

Dr. Milton Mueller
Georgia Tech School of Public Policy

Col. Suzanne Nielsen, Ph.D.
U.S. Military Academy

Dr. Hy S. Rothstein
Naval Postgraduate School

Dr. Bhavani Thuraisingham
The University of Texas at Dallas

Ms. Liis Vihul
Cyber Law International

Prof. Tim Watson
University of Warwick, UK

Prof. Samuel White
Army War College

CREATIVE DIRECTORS
Sergio Analco
Gina Daschbach

LEGAL REVIEW
Courtney Gordon-Tennant, Esq.

PUBLIC AFFAIRS OFFICER
Maj. Lisa Beum

KEY CONTRIBUTORS

Clare Blackmon, Nataliya Brantly, Kate Brown, Neyda Castillo, Erik Dean, Debra Giannetto, Anton Hubbard, Col. Michael Jackson, Lance Latimer, Alfred Pacenza, Diane Peluso, Michelle Marie Wallace

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

SUBMISSIONS
The Cyber Defense Review
welcomes submissions at
mc04.manuscriptcentral.com/cyberdr

WEBSITE
cyberdefensereview.army.mil

The Cyber Defense Review (ISSN 2474-2120) is published by the Army Cyber Institute at West Point. The views expressed in the journal are those of the authors and not the United States Military Academy, the Department of the Army, or any other agency of the U.S. Government. The mention of companies and/or products is for demonstrative purposes only and does not constitute endorsement by United States Military Academy, the Department of the Army, or any other agency of the U.S. Government.
© U.S. copyright protection is not available for works of the United States Government. However, the authors of specific content published in The Cyber Defense Review retain copyright to their individual works, so long as those works were not written by United States Government personnel (military or civilian) as part of their official duties. Publication in a government journal does not authorize the use or appropriation of copyright-protected material without the owner's consent.
This publication of the CDR was designed and produced by Gina Daschbach Marketing, LLC, under the management of FedWriters.
The CDR is printed by McDonald & Eudy Printers, Inc. ∞ Printed on Acid Free paper.

INTRODUCTION

SENIOR LEADER PERSPECTIVE

RESEARCH ARTICLES

RESEARCH NOTE

BOOK REVIEW

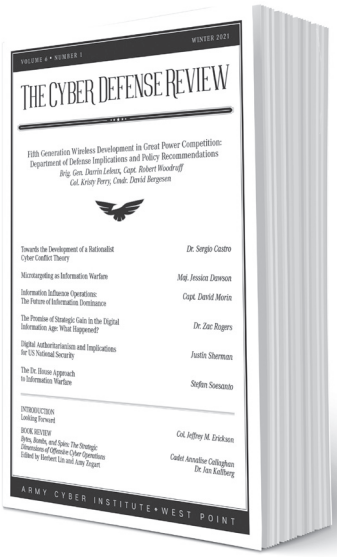
The Cyber Defense Review

Introduction

VOL. 6 ◆ NO. 1

The Cyber Defense Review: Looking Forward

Colonel Jeffrey M. Erickson



As 2020 was ending, there was a good deal of "Glad this year is over!" humor across social media. Of course, 2020 was unique with a global pandemic, but I think we all realize that the difference between the last day of 2020 and the first day of 2021 was not much more than a single rotation of the Earth. Most of the conditions between one moment to the next have not substantially changed.

However, one thing that is changing is an increasing awareness of the threat of cyber infiltration and attacks. Being a U.S. Presidential election year served as a focal point for cybersecurity, despite little evidence of disruption through electronic means. Instead, we learned of infiltration across vast amounts of industry and the United States Government (USG).

The SolarWinds attack highlighted the pervasiveness of threats across organizations and networks. With over 250-plus government agencies and businesses affected, it is becoming clear that no organization is safe.[1] Considering the reports that the intrusion occurred as early as March/April 2020, it highlights the challenges of maintaining and defending networks. Simply put, by the time you discover the threat, it is already too late. Instead, increasing situational awareness ahead of time becomes even more critical.

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

1 D. Sanger, N. Perlroth, and J. Barnes, "As Understanding of Russian Hacking Grows, So Does Alarm," *The New York Times*, accessed January 6, 2021, https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html.

Colonel Jeffrey M. Erickson is the Director of the Army Cyber Institute at the United States Military Academy (USMA) located at West Point, New York. As Director, COL Erickson leads a 60-person, multi-disciplinary research institute focused on expanding the Army's knowledge of the cyberspace domain. He began his Army career as an Armor officer before transitioning to the Simulation Operations functional area, where for the last 15 years, he has been using simulations to train from the individual to the Joint and Combatant Command levels. He has a B.S. in Computer Science from the United States Military Academy, an M.S. in Management Information Systems from Bowie State University, and an M.S. in National Resource Strategy from the Eisenhower School (formerly the Industrial College of the Armed Forces). His fields of interest are simulations for live-virtual-constructive training, testing, and wargaming.

To that end, *The Cyber Defense Review* Winter edition presents a great collection of authors from across the global community. We hope that these articles will expand your understanding of the challenges we face with respect to cyberspace while also providing recommendations on how to mitigate these issues.

With respect to new technologies, our Leadership Perspective article "Fifth Generation Wireless Development in Great Power Competition" by Brig Gen Darrin Leleux, CAPT Robert Woodruff, COL Kristy Perry, and CDR David Bergesen provide relevant thoughts and recommendations concerning the implementation of 5G technology. The authors identify the opportunities and risks associated with the 5G technologies by looking at the recommendations of the Defense Science Board, the Defense Innovation Board, and the European Commission. Through this analysis, the authors propose a potential whole-of-government approach in leading the implementation to mitigate security risks, both in and out of the USG.

In the area of Information Warfare/Operations, we have a diverse set of articles. The Army Cyber Institute's MAJ Jess Dawson provides a critical perspective on the increasing threat of micro-targeting and how the evolving surveillance economy poses a real threat to the mission readiness of military members and their families. She posits that this is becoming a potential force protection issue and will only increase unless the Department of Defense implements some mitigations. Dr. Zac Rogers (Flinders University, Australia) looks to fill the gap between information operations and cognitive warfare/security by looking to define the terms and their impact on warfare in his article "The Promise of Strategic Gain in the Digital Information Age: What Happened?" For a different perspective, Stefan Soesanto (ETH Zurich) provides a unique approach to Information Warfare, using the popular medical drama "House." Adopting the skeptical and blunt approach of Dr. House may counter

the frustratingly fast disinformation and misinformation campaigns of bad actors by focusing on their networks and not on their content. Finally, in our high-velocity Research Note section, CPT David Morin (93d Signal Brigade) proposes that the construct of Information Influence Operations (IIOs) will provide an approach to exert influence and strategic messaging within cyberspace.

At a strategic/state level, Dr. Sergio Castro (Instituto de Ciberdefensa, Mexico) proposes a model that correlates cyber operations and their broader strategic consequences in his article "Towards the Development of a Rationalist Cyber Conflict Theory." In "Digital Authoritarianism and Implications for US National Security," Justin Sherman (non-resident fellow at the Atlantic Council's Cyber Statecraft Initiative) highlights how the increasing use of technology by malicious state authorities can be used to entrench state power, increase domestic surveillance, and insulate regimes from external cyberattacks.

For those looking to expand their cyber library, United States Military Academy Cadet Annalise Callaghan and Dr. Kallberg from the ACI, provide a review of *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations* (ed. Herbert Lin and Amy Zegart). The anthology delivers some unique perspectives from a variety of authors on various facets of cyberspace.

As a reminder, our next issue will be a COVID-19 special edition (Spring 2021), capturing some thoughts on the pandemic's impact in the cyberspace environment, from our homes to our businesses to the highest levels of government.

Additionally, while the future of conferences remains uncertain, I encourage CDR readers to consider attending NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) Conference on Cyber Conflict (CyCon), occurring 25-28 May 2021 in Tallinn, Estonia. We hope to see you there (even virtually).

In conclusion, as we look forward to 2021, I like to use the term "skeptical optimism." This can best be defined as "seeing the glass as half full, but always brainstorming ways to fill the glass to the top."[2] Regardless of what 2021 brings, I am hopeful that the continuing dialogue of cyber professionals will continue to push the community to fill that glass.

2 L. Stevens, "On Being a Skeptical Optimist," accessed January 6, 2021, https://www.thinksplendid.com/blog/optimism-in-business.

The Cyber Defense Review

Senior Leader Perspective

Fifth Generation Wireless Development in Great Power Competition

Department of Defense Implications and Policy Recommendations

Brigadier General Darrin Leleux
Captain Robert Woodruff
Colonel Kristy Perry
Commander David Bergesen

ABSTRACT

The advent of fifth generation (5G) wireless technology represents new global opportunities and risks that must be considered in the context of reemerging long-term strategic competition with China and Russia, which are intent on shaping a world consistent with their authoritarian models.[1] To deal with this challenge, several bodies – notably the Defense Science Board (DSB), the Defense Innovation Board (DIB), and the European Commission (EC) – have recently offered recommendations on how leaders of large organizations, including nation-states in the case of the EC recommendations, should adopt and field this new communications technology. This article evaluates these recommendations to synthesize a possible way ahead for the Department of Defense (DoD); however, DoD cannot do this alone. A whole-of-nation approach is required for the United States to lead global change and gain the "first-mover" advantage.[2]

INTRODUCTION

The development of fifth generation (5G) wireless technology security is critical for United States (US) national defense and economic security. 5G technology represents a leap forward in the speed and volume of data transmission, as well as a drastic reduction in communication latency, which enables new technologies and operational methodologies. It also has the potential to improve security by interlinking intelligence, surveillance, reconnaissance, and command and control systems by delivering information in real time.[3] The Department of Defense (DoD) must have a strong voice in the development and implementation of 5G technology and associated security measures in order to prevent its adversaries from conducting intellectual property theft, interfering with DoD operations, and compromising the security of DoD personnel, information, equipment, and operational

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

Brigadier General Darrin Leleux, U.S. Air Force, is currently serving as Deputy Director of the Electromagnetic Spectrum Operations Cross-Functional Team. He was commissioned through the Reserve Officer Training Corps (ROTC) and earned a Bachelor of Science in Electrical Engineering degree from the University of Southwestern Louisiana in 1989, a Master of Science in Computer Engineering from the University of Houston at Clear Lake in 1998, and a Doctor of Philosophy in Electrical Engineering from Rice University in 2002. Prior to his current assignment, General Leleux served as Deputy Director of Strategy, Defense and Capabilities in the Office of the Secretary of Defense for Cyber Policy.

capabilities that will rely on 5G. Since this is a whole-of-nation issue, the U.S. Government (USG) must deliberately incorporate 5G security into conversations with foreign partners, industry, and DoD to evaluate carefully the role of 5G technology in its own, as well as its coalition partners,' communication architectures and operational capabilities.

It is critical that partner governments and domestic/international industries understand the potential risks of using 5G hardware and software from companies such as Huawei and ZTE – both Chinese-owned companies. Beyond the price of initial network investment, leaders should also consider the costs incurred through security compromises and remediation efforts – such as loss of capital, intellectual property, or markets – if strong security is not built into 5G systems and network segments from the beginning. The USG should lead a national effort and continue to be engaged in the establishment of 5G standards which will require the extensive and persistent presence in standard-setting organizations and bodies such as the 3rd Generation Partnership Project (3GPP) and the Institute of Electrical and Electronics Engineers (IEEE). Furthermore, since part of the electromagnetic spectrum that will be utilized for 5G overlaps with DoD and USG public safety frequencies, creative and viable new approaches should be developed with industry to operate dynamically within these specific cooperation segments of the wireless spectrum. Finally, it is critical for global scale 5G systems to be built to the highest security standards to safeguard intellectual property, intelligence, information, and equipment not only in DoD but throughout the US.

In this article, we review and analyze the 5G recommendations made by different organizations to identify commonalities and differences that may be useful in synthesizing a way forward for DoD. We evaluated recommendations by the Defense Innovation Board (DIB), the Defense Science Board (DSB),

Captain Robert Woodruff, U.S. Navy, is currently serving as Information Operations Branch Head at NATO Maritime Command (Headquarters Allied Maritime). He was commissioned through ROTC at Texas A&M University at Galveston in 1999. He earned a Bachelor of Science degree in Maritime Systems Engineering degree from Texas A&M University at Galveston and a Master of Arts in National Security and Strategic Studies from the U.S. Naval War College in 2011. Prior to his current assignment, Captain Woodruff served as Executive Officer at Navy Cyber Warfare Development Group and Deputy Commander of Task Force 1090.

and the European Commission (EC). These organizations offered recommendations in 2019 for large organizations such as DoD and the European Union (EU) to consider when adopting and fielding this new communications technology. We evaluate each of their recommendations in turn with an emphasis on those offered by the DIB, and then synthesize a possible way ahead for DoD.

ANALYSIS OF DEFENSE INNOVATION BOARD RECOMMENDATIONS

The DIB was created in 2016 to bring the technological innovation and "best practices" of Silicon Valley to the US military.[4] They completed a study on "The 5G Ecosystem: Risks & Opportunities for DoD" and published their recommendations in April 2019.[5] The study offered three unclassified recommendations for DoD related to spectrum management, preparing for a "post-Western" wireless ecosystem, and developing trade and supply chain mitigations. In the next few paragraphs, we analyze the first two recommendations and offer ideas to advance the thinking on these topics. The third recommendation, while extremely important, is not included in our analysis as this has been covered extensively in other articles and the news media.

> Recommendation #1
>
> DoD needs a plan for sharing sub-6 GHz spectrum to shape the future 5G ecosystem, including an assessment of how much and which bandwidths need to be shared, within what time frame, and how that sharing will impact DoD systems.

Spectrum sharing and shaping the 5G ecosystem is much larger than just a DoD problem. Collaboration between the USG and the commercial sector is critical to effectively innovate and develop a national plan. The Trump administration recognized 5G as a next-generation technology in its 2017 National Security Strategy, highlighting the criticality of the US becoming a first mover and global leader. The administration designated

Colonel Kristy Perry, U.S. Army, is currently serving in United States Cyber Command (USCYBERCOM). She was commissioned through ROTC at Southwest Missouri State University in Springfield in 2000. She earned a Bachelor of Science in Business degree from Southwest Missouri State University and a Master of Science in International Relations from North Carolina State University in 2009. Prior to her current assignment, Colonel Perry served as an Army War College Fellow at the National Security Agency.

the US private sector to lead national efforts in 5G developments.[6] In October 2018, President Trump issued a presidential memorandum to create a National Spectrum Strategy.[7] In April 2018, the National Telecommunications and Information Administration (NTIA) announced plans to develop a collaborative strategy, including spectrum sharing, selling, and development of mid- and high-frequency bands.[8] The National Spectrum Strategy team is comprised of federal and non-federal stakeholders, in addition to public-private partnerships, relying on a flexible spectrum management regulatory model and research establishing a comprehensive set of immediate and long-term requirements[9]. As then NTIA Administrator and leader of the strategy development, David J. Redl stated, "While commercial needs are extensive, we must balance that against government's expanding needs for national defense, public safety, aerospace, and other vital missions."[10] As technology evolves, the spectrum strategy must focus on being agile, collaborative, inclusive, and well-researched and tested. The DoD Spectrum Policy Office under the DoD Chief Information Office (CIO) released a spectrum strategy in 2014; however, the strategy is exclusive to DoD, and, like Redl, recognized the need for collaboration, greater efficiency, flexibility, and spectrum sharing at the national level.[11] More recently, the Secretary of Defense released a new Electromagnetic Spectrum Superiority Strategy in 2020 calling for DoD to lead the way in the development of dynamic spectrum sharing technologies and techniques. Furthermore, DoD awarded a five-year $2.5 billion Spectrum Forward contract designed to accelerate the development and eventual deployment of new technologies including dynamic spectrum sharing for 5G systems.

DoD Sharing of the Sub-6 Gigahertz (GHz) Spectrum (Sub-6)

The sub-6 was designated as the international standard for wireless spectrum usage at the International Telecommunications Union's World Radiocommunication

Commander David Bergesen, U.S. Navy, is currently serving as the Department Head for Navy Intelligence Policy, Requirements, and Wholeness at U.S. Fleet Forces Command. He was commissioned through ROTC at the University of Arizona in 1998. He earned a Bachelor of Arts in Spanish Language and Linguistics degree from the University of Arizona, and a Master of Science in Cyber Systems and Operations from the Naval Postgraduate School in 2014. Prior to his current assignment, Commander Bergesen served as the Ship's Intelligence Officer onboard the USS *John C. Stennis* (CVN-74).

Conference in 2015. However, in the US, sub-6 is primarily managed and utilized by DoD and federal government agencies, leaving limited options for industry development in that range. The DIB recommended that DoD establish a spectrum-sharing plan. US spectrum segmentation and utilization require a holistic approach with national collaboration. Presently, however, there is insufficient collaboration across the private sector and federal agencies to clearly understand the operational risks, costs, required policy changes, and timelines associated with such spectrum sharing. As stated by the Cellular Telecommunications and Internet Association (CTIA) representing the wireless communications industry in the US, "DoD must prepare itself for that future operating environment by focusing on co-existing, if not explicitly sharing, with civil 5G operations in those bands of spectrum."[12] Spectrum usage varies substantially by frequency bands, spread across a diverse set of organizations and functions, further highlighting the need for collaboration.

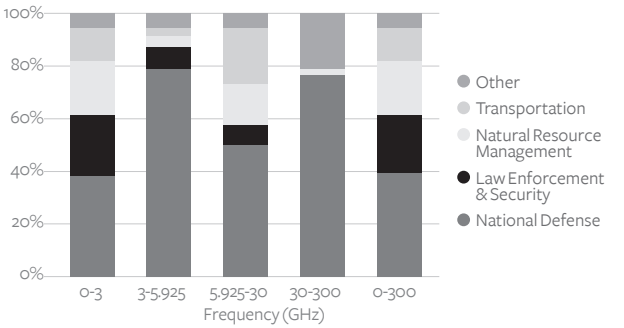


Figure. Federal Government Spectrum Usage[13]

Sub-6 vs. Millimeter Wave (mmWave)

Defense systems, public safety, aerospace and maritime agencies, and private industry operate across various segments of the electromagnetic spectrum; therefore, understanding the capabilities and limitations of the various spectrum bands is essential. 5G wireless systems are designed to operate within two distinct frequency regions: sub-6 and mmWave. The sub-6 band

operates at lower frequencies with corresponding longer wavelengths, while the mmWave operates at higher frequencies with significantly shorter wavelengths. Lower-frequency transmissions such as with sub-6 technologies do not attenuate as readily as higher-frequency ones used by mmWave technology and can achieve greater ranges. However, higher frequencies do offer increased transmission capacity (including more bandwidth available for security overhead), decreased latency, and considerably higher speeds. 5G wireless technology operating in the mmWave segment has been shown to transmit data up to 20 times faster than fourth generation (4G) wireless technology operating in the sub-6 band.[14] Quite significantly, though, the shorter wavelengths of signals in the mmWave bands are more susceptible not only to attenuation but to atmospheric (including moisture and airborne particulates) and physical obstructions (such as concrete, steel, or even trees). Practically, this means degraded signal penetration and possible signal interruption in congested urban environments. 5G systems operating in the sub-6 band would require fewer cell towers or base stations, making sub-6 implementation more cost-effective for telecommunications providers and, therefore, customers.

The international designation of sub-6 as the global standard has led international telecommunications manufacturers (including Chinese firms Huawei and ZTE) to develop hardware that operates primarily within the sub-6 range. As a result, many nations seeking to upgrade to 5G will opt for sub-6, as doing so will require fewer component upgrades while offering increased compatibility within existing 4G infrastructures. This, in turn, will enable more efficient transitions to 5G technology with a lower initial overhead, despite lower speed and bandwidth than mmWave technology.

While the physical characteristics of signals over a continuous range of frequencies change in a continuous manner, it is helpful to consider the advantages and disadvantages of signals within both the sub-6 and mmWave bands. The National Spectrum Strategy must develop an approach to benefit from each. To compete in the international development of 5G technology, the US must direct immediate attention to innovation in sub-6 and work on longer-term mmWave solutions for global markets. The near-term approach for sub-6 should include not only sharing and spectrum lease options but also auctioning of sub-6 spectrum where feasible. Due to the propagation issues with shorter wavelength signals, additional research and development time is required to make mmWave 5G globally viable. Lack of innovation in the sub-6 band would put the US behind 5G innovations by peer competitors that have deliberately focused on sub-6.

Spectrum Auctioning

In December 2018, the Federal Communications Commission (FCC) hosted the largest spectrum auction to date.[15] FCC efforts were focused on selling sub-6 to non-federal entities prioritizing 5G innovations. Although auctioning spectrum is not a new practice, the selling of the sub-6 spectrum was extremely limited in the past. While the FCC shifted to auction portions of the sub-6 spectrum, the time required to transition awarded bands fully is between five and

ten years. With the anticipation of China delivering 5G capabilities soon, the current transition timelines require an immediate upgrade. The Facilitate America's Superiority in 5G Technology (5G FAST) plan is the FCC's comprehensive strategy to make the 5G spectrum open to industry more rapidly, though it may not be fast enough.[16] Sub-6 is the immediate priority, but the 5G FAST plan is inclusive of all bands, recognizing the benefits of leveraging commercial innovation and hybrid solutions within the National Spectrum Strategy.[17] Reallocation of spectrum is both costly and time-consuming. A March 2012 NTIA study indicated that the cost to incumbent users in the federal government for reallocation of just one band of interest (1755-1850 MHz) was estimated to be $18 billion. This reallocation would also require ten years to relocate most of the systems and new federal access to two spectrum bands to accommodate relocated systems.[18] To remain competitive with China, sharing and lease options provide a more immediate solution.

Spectrum Sharing/Leasing

"Sustainable spectrum use is not a one-size-fits-all proposition but a blend of methods for a variety of needs," explained Dr. Matthew Clark, an engineering specialist at The Aerospace Corporation, "and the goal of spectrum sharing systems isn't simply to avoid interference by accounting for every possible sharing scenario but to provide practical services." Spectrum sharing enables multiple systems to use the same RF spectrum. DoD risks inherent to spectrum sharing are serious as they include the potential loss of operational security (OPSEC), loss of effective cybersecurity in reducing malicious activity, difficulty in safeguarding intellectual property, and the potential for RF interference.[20] Spectrum is the "maneuver space behind nearly all operations and spectrum innovation is an important part of how we (DoD) fight," former DoD Deputy CIO, Maj Gen Sandra Finan, stated.[21]

Although risk is inherent in 5G development, DoD also stands to benefit from industry innovations by gaining spectrum modeling and simulation tools, leveraging artificial intelligence, and allowing DoD traffic to "hide in plain sight."[22] DoD understands the need to collaborate and is currently participating in multiple collaboration and research efforts to support the sharing of spectrum, with a "trust but verify" approach.[23] The National Spectrum Consortium and the National Advanced Spectrum and Communications Test Network (NASCTN) is a multi-agency chartered partnership providing testing, modeling, and analysis to develop spectrum-sharing technologies and inform policy.[24] NASCTN was created in 2015 and comprises the National Institute of Standards and Technology (NIST), the NTIA, the DoD, the National Aeronautics and Space Administration (NASA), the National Science Foundation (NSF), and the National Oceanic and Atmospheric Administration (NOAA).[25]

The FCC and the NTIA both have responsibility and authority to allocate and license use of the spectrum; though each organization performs unique roles, they do coordinate spectrum issues. The Interdepartment Radio Advisory Committee (IRAC) – an entity within the NTIA – is responsible for coordinating and adjudicating spectrum issues on behalf of all government

agencies, including the DoD. The FCC, while not a voting member of the IRAC, is chartered to coordinate all non-federal spectrum-related actions with the IRAC (and vice versa). It is therefore important to recognize that DoD must coordinate all its spectrum needs through the IRAC. Additionally, the Department of State, in coordination with the FCC and NTIA, is responsible for US participation in the ITU-sponsored World Radio Conferences, where worldwide allocations are considered.

It is notable that the NTIA developed a Spectrum Sharing Innovation Test-Bed pilot program focused on the feasibility of spectrum sharing across federal and non-federal agencies. The test bed is comprised of academia, industry, and government agencies and targets sensing, geo-tagging, and location on mobile radio systems.[26] The focus of the test bed is to evaluate equipment characterizations and capabilities followed by a field operational evaluation.[27] This aligns with the "test but verify" concept to find ways to collaborate while mitigating risk.

As recommended by the DIB, DoD must plan for sharing the sub-6 spectrum and assessing bandwidths to be shared, while understanding the impact to DoD systems; however, DoD cannot do it alone. Executing a national spectrum strategy that protects both national and lower-level security concerns will take a collaborative effort. The 5G ecosystem is going to revolutionize global communications; DoD operations, networks, and command and control systems will also benefit from the innovation. It is essential that flexibility, agility, and security are implemented within the collaborative design phase.[28]

> Recommendation #2
>
> DoD must prepare to operate in a "post-Western" wireless ecosystem. This plan should include R&D investments toward system security and resilience on an engineering and strategic level.[29]

Recommendation #2 suggests that China will have a great advantage if it is the first to deliver 5G infrastructure and devices globally, gaining first-mover advantage. The DIB reports that "first-mover advantage is particularly pronounced in wireless generation transitions because the leader can set the foundational infrastructure and specifications for all future products."[30] Many countries will already be beholden to Chinese products when establishing 5G wireless technology networks due to component price and availability of components, as well as compatibility with proprietary interfaces of their current 4G infrastructures or network devices sourced from China.[31]

Chinese companies such as Huawei and ZTE Corporation present critical security risks as they are state-owned enterprises linked to the government. This has the potential to create a global information technology (IT) infrastructure susceptible to Chinese predatory practices, such as intellectual property theft and Chinese-mandated technology transfers creating many security vulnerabilities.[32] China's government has usurped physical and intellectual property, creating an advantage in the information space by exploiting data through creating back door

vulnerabilities within hardware and/or software. In 2019, many Chinese IT companies were implicated in nefarious cyber activities and directly linked to China's government.[33] This linkage can arguably be considered part of the culture as Chinese Law Articles 14 and 17 (National Intelligence Law, enacted June 27, 2017) indicate that Chinese companies have an active role in supplying information and/or access to the state.[34] This culture has provided state-sponsored leverage to make China a peer competitor and adversary of the US, at large, not just DoD.

Security

Security standards provide the basic parameters to create a secure environment across 5G wireless networks and are vital to maintain the confidentiality, integrity, and availability of US data as it traverses through information networks. To protect US data and systems, several improvements to current systems need to be pursued, including policy changes to ensure only secure equipment is used in USG systems, the development of quantum-resistant cryptography, improvement of software-defined networking technologies, and tighter controls over supply chain management. All these changes must be carefully orchestrated to work in concert with each other across all government agencies and industry partners.

Policy and implementation of cryptographic standards are required for global security. US policy protections restrict companies that are non-compliant with current IT security standards from providing equipment for the 5G infrastructure; however, the same standards do not apply to allied countries.[35] These cryptographic standards are being developed by NIST under the U.S. Department of Commerce for use by non-national security federal information systems. Though these systems are for non-national security systems, they could be reviewed or adjusted for applicability to national security systems or critical infrastructure, as well.[36] Smart design of the 5G infrastructure to use these new cryptographic standards would ensure that over the next decade, as the US experience with 5G wireless technology increases and its security is improved, the risk of information theft and unintended decryption remains low. A primary issue is finding a standard that will not impose excessive latency, thereby reducing the benefit of using the new 5G wireless technology. Regardless of the security approaches taken, the US should ensure persistent research and development efforts in security and resilience for the network while operating both in the US and internationally.

Resilience

Deliberate USG planning and action must be taken to ensure resilience when using 5G wireless systems. Two required actions to ensure a cyber-resilient methodology for US 5G wireless systems are: (1) develop better capabilities to observe anomalies or attacks in real time, and (2) improve the ability for cyber defenders to act at the speed of relevance.

USG systems must be able to determine that an attack, malicious event, or exploitation is in progress to take timely actions to ensure system resilience. To identify early warning of an anomaly or attack, US entities must understand their standard day-to-day environment,

sense that something is out of the ordinary, and determine what is happening across the digital domain.[37] Additionally, as DoD implements equipment that can leverage the 5G wireless infrastructure, military communications operators need to be trained and have the right tools to detect outside influence. Once an attack is identified, the more difficult task is attributing the activity to a malicious actor and then identifying the attack vector. To accomplish this, DoD should improve training programs for its cyber warriors and develop tools that can detect anomalies and potentially take the first steps in countering cyber-attacks. To help identify attack vectors and determine where an attack came from, new authorities or adjustment to current authorities may be required, especially if autonomous actions are incorporated into these systems.

Once a malicious act is identified, military operators must take timely action to stop the event. Finding or identifying the attack vector and stopping the inflow or outflow of data through system manipulation are key. To ensure resilience, military operators should be able to switch between 5G wireless and other secure wireless standards as seamlessly as possible.[38] Regardless of the standards, the key to resilience is having the ability to continue combat operations with or without an available network, albeit with reduced functionality. DoD should continue practicing and exercising scenarios either to maneuver or determine alternate means to remain combat-effective in contested, degraded, or denied electromagnetic spectrum environments. These competitive environments in which the cyber domain is contested are where victory in the next war will most likely be determined.

ANALYSIS OF DEFENSE SCIENCE BOARD RECOMMENDATIONS

Established in 1956, the DSB is a committee of civilian experts appointed to advise DoD on scientific and technical matters. The DSB completed a recent six-month Quick Task Force on "Defense Applications of 5G Network Technology."[39] The Task Force's stated objective was "to define a path for potential DoD 5G adoption that mitigates supply chain risk, establishes spectrum co-existence procedures and revamps existing communication infrastructure." The Task Force published its findings and recommendations in June 2019. The report offered the following ten recommendations:

1. Adopt 5G for military use in lightly contested environments.
2. Develop a secure 5G system for contested environments and critical applications.
3. Create test beds for exploring innovative use cases.
4. Stand up a telecommunications security program.
5. Develop a DoD 5G supply chain management strategy.
6. Create a program for "vulnerability analysis."
7. Develop and execute a three-year 5G+ Science and Technology Roadmap.

8. Develop a 5G+ Standards Engagement Plan.
9. Establish a new bi-directional spectrum-sharing paradigm.
10. Accelerate mmWave technology development and transition.

The DIB and DSB recommendations disagree on which portion of the spectrum to focus development (i.e., sub-6 or mmWave). The DIB report acknowledged that "the rest of the world is focused on building out sub-6 infrastructure, with China in the lead." Since DoD will have to operate overseas, it will "ultimately have to learn to operate on that sub-6 infrastructure, regardless of how the US chooses to implement 5G domestically." While the DSB recommendation acknowledges that DoD must be prepared to operate in a contested environment, recommendation #10 clearly focuses on accelerating mmWave technology "as the first priority" over sub-6 bands. Additionally, the DSB recommends that the Defense Advanced Research Projects Agency (DARPA) refine propagation models and investigate the feasibility of adapting 5G fixed mmWave technology to mobile, airborne, and satellite links. It also recommends that DARPA continue to track the development of 5G mmWave technology and create new opportunities for advancement. As stated previously, DoD in partnership with other USG agencies and industry must develop across the spectrum, while prioritizing efforts to sub-6. It also recommends building out mmWave technologies to provide both agility and flexibility of use throughout all environments. Finally, the DSB recommendations agree that a frequency sharing program must be implemented.

The difference in focus between the DIB and DSB recommendations for development of the sub-6 vs. mmWave bands highlights one of the fundamental considerations in 5G policy development, i.e., how much focus should be given to the sub-6 bands which have lower overall potential from a technical perspective. Given its early development by the international community, it has the potential to be ubiquitous soon, particularly among US allies and partners. Due to advantages and disadvantages previously discussed in this article, DoD must take a two-pronged approach ensuring relevance and interoperability in the near term by innovating in the sub-6 space as well as spectrum dominance in the future by innovating in the mmWave space. DoD should not focus solely on one band over the other but should take a balanced approach considering all advantages and disadvantages of these two bands within the spectrum. As of this writing, the US has made and is making allocations for 5G in distinct bands that fall into the sub mmWave bands as well as above, in fact some considerably higher. The 5G FAST Plan of the FCC details the specific bands.

ANALYSIS OF EUROPEAN COMMISSION RECOMMENDATIONS

The third set of recommendations examined were proposed by the EC in March 2019, offering a common EU approach to 5G. The recommendations were published in the article "European Commission recommends common EU approach to the security of 5G networks."[40] The recommendations leverage a December 2018 EU Cybersecurity Act that was agreed to by the European

Parliament, the European Council, and the European Commission. Unlike the DIB and DSB recommendations, the EC recommendations focus on the process of developing 5G standards, strategies, and security controls rather than considerations of the specific technologies. In synthesizing a way forward for DoD, consideration should be given both to the processes associated with developing 5G policies and to the technology's advantages and disadvantages.

The EC recommendations provide a concrete path forward for EU member countries and the EU writ large. Many of the recommendations of the Commission potentially may be applied to DoD. Adapting these recommendations to DoD focuses on developing a central coordination and information-sharing network that requires DoD components to develop component-level 5G risk assessments and update existing cybersecurity requirements and contracting mechanisms to consider 5G technology. Additionally, these recommendations would standardize mitigating 5G security controls including, but not limited to, certification requirements, tests, security controls, and the identification of products or suppliers that are considered potentially non-secure. These recommendations would also develop and mandate DoD 5G cybersecurity certification frameworks for all DoD 5G digital products, processes, and services.

SUMMARY OF DOD RECOMMENDATIONS

After reviewing and analyzing the recommendations made by the organizations discussed in this article, we offer the following eight recommendations, which include consideration for both process and technology as a way forward for DoD:

1. **Create a DoD 5G Coordination Group** – Establish a senior DoD-wide 5G coordination group with representation from across the Department to implement the recommendations listed below.
2. **Create a 5G Cybersecurity Information Sharing Network** – Develop a DoD-wide 5G cybersecurity information-sharing network.
3. **Develop a 5G Cybersecurity Threat Assessment** – Immediately complete a 5G cybersecurity threat landscape assessment that will support DoD agencies in completing their DoD component-specific risk assessments.
4. **Develop DoD Component-Level 5G Risk Assessments** – Using NIST Special Publication 800-37 (Guide for Applying the Risk Management Framework) as a guide, mandate that each DoD component conduct a component-level risk assessment of 5G network infrastructures in the near term including, but not limited to, identifying threats, vulnerabilities, and mitigating security controls.
    a. Include technical risks linked to the behavior of suppliers or operators, including those from China, Russia, North Korea, and Iran.
    b. DoD agencies would then submit threat assessments to the DoD-wide 5G coordination group to identify common threats.

5. **Update Existing Cybersecurity Requirements for 5G** – Mandate that each DoD component update existing cybersecurity requirements to include 5G network providers and include conditions for ensuring the security of DoD networks especially, when granting rights of use for RF in 5G bands. Updated cybersecurity requirements should include the following:
    a. Reinforced contract obligations on suppliers and operators to ensure the security of their 5G networks, and
    b. The right of DoD components to exclude companies from their 5G suppliers and operators for national security reasons if they do not comply with DoD 5G standards.
6. **Develop a Coordinated DoD 5G Risk Assessment** – DoD component-level 5G risk assessments will be a central element in building a coordinated DoD 5G risk assessment. The DoD-wide 5G coordination group should implement the following:
    a. Assess the effects of both DoD-wide and component-level recommendations to determine whether there is a need for further action,
    b. Develop standardized 5G security controls which should include, but are not limited to, certification requirements, tests, security controls, and the identification of products or suppliers that are considered potentially non-secure, and
    c. Develop and mandate DoD 5G cybersecurity certification frameworks for all 5G digital products, processes, and services.
7. **Develop DoD 5G Contract Requirements** – Develop specific DoD security requirements for contracts related to 5G networks, including mandatory requirements to implement 5G cybersecurity certification frameworks. Additionally, DoD should consider segmenting off, or deliberately routing around, networks or network segments that do not follow DoD 5G cybersecurity certification standards.
8. **Develop DoD 5G Policy** – Develop a DoD policy that requires operators take technical and organizational measures to manage appropriately the risks posed by security of 5G networks and services.

RECENT PROGRESS

Since the original writing of this article in the summer of 2019, significant progress has been made in advancing US 5G policy.

First, Congress passed the "Secure 5G and Beyond Act of 2020" on March 23, 2020. It requires development of a national strategy, to be known as the National Strategy to Secure 5G and Next Generation Wireless Communications, which shall ensure the security of 5G wireless communications systems and infrastructure within the US; assist mutual defense treaty allies, strategic partners, and other countries in maximizing the security of 5G systems and infrastructure;

and protect the competitiveness of US companies, privacy of US consumers, and integrity of standards-setting bodies.

Second, the President approved, and the White House published on March 23, 2020, a "National Strategy to Secure 5G of the United States of America." This document lays out four lines of effort:

1. Facilitating domestic 5G rollout.
2. Assessing the risks and identifying core security principles for 5G infrastructure.
3. Managing the risks to our economic and national security from the use of 5G infrastructure.
4. Promoting responsible global development and deployment of 5G infrastructure.

Third, the Federal Communications Commission established the 5G FAST Plan to implement the President's policy. This plan entails taking action to make additional spectrum available for 5G services, updating infrastructure policy and encouraging the private sector to invest in 5G networks, and modernizing outdated regulations to promote the wired backbone of 5G networks and digital opportunity for all Americans. The plan addresses each of the low, mid, and high bands as well as the potential bands for unlicensed allocation. It addresses the specific bands that the Commission has already allocated (and in some cases auctioned), or intends to allocate, for 5G services. The plan also addresses FCC policies for updating infrastructure policy, particularly for small cells. Finally, the plan addresses FCC intentions to modernize regulations pertaining to 5G backhaul and digital opportunities for Americans. This includes requirements for supply chain integrity and national security considerations. It emphasizes the importance of backhaul infrastructure as it is crucial for small cell connectivity to the rest of the network. Furthermore, the Commission recognized the import of integration of the radio access network (the basis for 5G) with the backhaul network, which couples with a switching network to form the basis of the overall communications network and architecture.

Fourth, a new initiative of industry and the FCC is worthy of note. The Commission has initiated an "Open Radio Access Network (RAN)" proceeding. An Open RAN, or Open Radio Access Network (O-RAN), is a concept based on interoperability and standardization of RAN elements including a unified interconnection standard for hardware and open-source software elements from different vendors. An O-RAN architecture integrates a modular base station software stack implemented on off-the-shelf hardware which allows baseband and radio unit components from discrete suppliers to operate together seamlessly. The O-RAN will most certainly contain important elements of the security stack as well.

Finally, the DoD has been advancing both doctrine and strategy to transition away from the traditional consideration of electromagnetic warfare (EW) as separable from spectrum management to a unified treatment of these activities as Electromagnetic Spectrum Operations (EMSO). Recent examples of this include the publication of the new Joint Publication 3-85

titled Joint Electromagnetic Spectrum Operations (JEMSO) in May 2020 and the October 2020 release of the new Electromagnetic Spectrum Superiority Strategy aligned with the 2018 National Defense Strategy. In addition to calling for DoD to lead the way in the development of dynamic spectrum sharing technologies and techniques, the Strategy addresses how DoD will "develop superior Electromagnetic Spectrum (EMS) capabilities; evolve to an agile, fully integrated EMS infrastructure; pursue total force EMS readiness; secure enduring partnerships for EMS advantage; and establish effective EMS governance to support strategic and operational objectives."

CONCLUSIONS

The innovation of 5G technologies will make a global impact on wireless communications, creating many opportunities and risks, with the advantage going to the first mover. Three diverse groups made assessments of the impact of 5G, focusing on recommendations to large organizations such as DoD and the EU. In this article, we reviewed and analyzed these recommendations to identify commonalities and differences that may be useful in synthesizing a way forward for DoD. We evaluated each of the recommendations in turn, then synthesized a possible way forward for DoD. Although we agree that DoD is critical to US national security, it cannot operate alone and a whole-of-nation approach is required. DoD, USG agencies, private industry, and US allies must collaborate to innovate at a speed exceeding that of their adversaries, especially China. Although positioning DoD to mitigate vulnerabilities in this new technology is critical, 5G technologies must be leveraged as an opportunity to improve national security by innovating across the entire spectrum with high security standards.

DISCLAIMER

The views expressed in this work are those of the authors and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense.

NOTES

1. Jim Mattis, *National Defense Strategy*, May 1, 2018, accessessed July 15, 2019, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.
2. Defense Innovation Board, 2019, "The 5G Ecosystem: Risks and Opportunities for DoD," *defense.gov*. April 4, 2019, accessed July 19, 2019.
3. Ibid.
4. Wikipedia, *Defense Innovation Advisory Board*, accessed August 6, 2019, https://en.wikipedia.org/wiki/Defense_Innovation_Advisory_Board.
5. Defense Innovation Board, "The 5G Ecosystem: Risks and Opportunities for DoD."
6. Scott C. Brown, 2019, *Trump and FCC Outline Aggressive 5G Plan, will not Nationalize Networks*, April 12, 2019, accessed July 15, 2019, https://www.androidauthority.com/trump-fcc-5g-plan-975903/.
7. Paul Kirby, *DoD "All In" on Spectrum Sharing, Deputy CIO Tells Industry Group*, November 2, 2016, accessed July 19, 2019. https://blog.npstc.org/2016/11/04/dod-all-in-on-spectrum-sharing-deputy-cio-tells-industry-group/.
8. Tom Leithhauser, "Agencies, Private Sector Endorse Creation of a National Spectrum Strategy" *Telecommunications Report 84* (13): 2018, 25-28.
9. Paul Kirby, *DoD "All In" on Spectrum Sharing, Deputy CIO Tells Industry Group*.
10. Ibid.
11. Ibid.
12. Monica Alleven, "CTIA: DoD Report Fails to Reflect U.S. Standing in Race to 5G," May 3, 2003, accessed July 18, 2019, https://www.fiercewireless.com/wireless/ctia-dod-report-fails-to-reflect-u-s-standing-race-to-5g.
13. National Telecommunications and Information Administration, *How the Spectrum is Used*, https://www.ntia.doc.gov/book-page/how-spectrum-used.
14. Defense Innovation Board, "The 5G Ecosystem: Risks and Opportunities for DoD."
15. Scott C. Brown, *Trump and FCC Outline Aggressive 5G Plan, will not Nationalize Networks.*
16. European Commission, *European Commission recommends common EU approach to the security of 5G networks.* March 26, 2019, accessed August 6, 2019, https://europa.eu/rapid/press-release_IP-19-1832_en.htm.
17. Ibid.
18. Matthew A. Clark, "Aerospace Corporation," *aerospace.org,* November 2018, accessed July 19, 2019, https://aerospace.org/sites/default/files/2018-12/Clark_SpectrumSharing_12042018.pdf.
19. Ibid.
20. Ibid.
21. Paul Kirby, *"All In" on Spectrum Sharing, Deputy CIO Tells Industry Group*.
22. Defense Innovation Board, "The 5G Ecosystem: Risks and Opportunities for DoD."
23. Paul Kirby, *DoD "All In" on Spectrum Sharing, Deputy CIO Tells Industry Group*.
24. National Institute of Standards and Technology,*National Advanced Spectrum and Communications Test Network (NASCTN)*, accessed July 20, 2019, https://www.nist.gov/communications-technology-laboratory/nasctn.
25. Ibid.
26. National Telecommunications and Information Administration, U.S. Department of Commerce, *Specturm Sharing Innovation Test Bed*, accessed July 15, 2019, https://www.ntia.doc.gov/category/spectrum-sharing-innovation-test-bed.
27. Ibid.
28. Defense Innovation Board, "The 5G Ecosystem: Risks and Opportunities for DoD."
29. Ibid.
30. Ibid.
31. Ibid.
32. Mike Rogers, *The 5G Promise an the Huawei Threat; Big Brother is coming to your home via cheap Chinese goods*, January 29, 2019, accessed July 26, 2019. http://search.proquest.com.nduezproxy.idm.oclc.org/docview/2171790881?accountid=12686.

NOTES

33. 115th Congress, "Public Law 115-232 (John S. McCain National Defense Authorization Act For FY 2019), " NDAA 2019, Washington, DC; 116th Congress, "National Defense Authorization Act FY 2020." NDAA FY 2020, Washington, DC, Mike Rogers, *The 5G Promise an the Huawei Threat; Big Brother is coming to your home via cheap Chinese goods*, anuary 29, 2019, accessed July 26, 2019,http://search.proquest.com.nduezproxy.idm.oclc.org/docview/2171790881?accountid=12686; Jerry Hildenbrand, *How does a phone maker 'mistakenly' collect user data and ship it off to a server in China?* March 23, 2019, accessed July 25, 2019, https://www.androidcentral.com/how-does-company-nokia-or-oneplus-mistakenly-collect-user-data-and-ship-it-server-china.
34. Defense Innovation Board, "The 5G Ecosystem: Risks and Opportunities for DoD."
35. 115th Congress, "Public Law 115-232."
36. Lily Chen, Stephen Jordan, Yi-Kai, Moody, Dustin Liu, Rene Peralta, Ray Perlner, and Daniel Smith-Tone, 2016, *Report on Post-Quantum Crpytography*, NISTIR 8105, Washington, DC: National Institute of Standards and Technology (Department of Commerce). Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, Yi-Kai Liu, Carl Miller, et al. 2019, *Status Report on the FIrst Round of the NIST Post-Quantum Cryptography Standardization Process*, NISTIR 8240, Washington, DC: National Institute of Standards and Technology (Department of Commerce).
37. William Bryant, "Resiliency in Future Cyber Combat," *Strategic Studies Quarterly* (Winter 2015), 87-107.
38. Department of Homeland Security – Cybersecurity and Infrastructure Security Agency, *Overview of Risks Introduced by 5G Adoption in the United States*, July 31, 2019, accessed July 31, 2019, https://www.dhs.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf.
39. Craig Fields and Alfred Grasso, 2019, *Defense Applications of 5G Network Technology*. Report, Defense Science Board, Washington, DC: Defense Science Board Quick Task Force.
40. European Commission, “European Commission recommends common EU approach to the security of 5G networks.”

The Cyber Defense Review

Research Articles

Towards the Development of a Rationalist Cyber Conflict Theory

Dr. Sergio Castro

ABSTRACT

We believe there is a lack of a coherent Cyber Conflict Theory with adequate descriptive, predictive, and prescriptive capacities. We attribute this shortfall to the fact that the study of Cyber Conflict falls into two largely separate camps: International Relations and Information Security. International Relations experts study the phenomenon mostly using traditional conflict analysis models derived from the theory of conflict. On the other hand, Information Security experts focus on the tactical details of how cyber-attacks are conducted, but they are usually not involved in International Relations studies. The objective of this paper is to bridge this gap by linking the types of cyber-attacks both to their military consequences and their broader strategic consequences. To achieve this, we use Fearon's Bargaining Model of War to analyze the impact that offensive cyber operations have on the probability of winning a war, the cost of war, and the risk of war. We identify three types of cyber operations: Extraction, Modification, and Denial of Service. Our model shows that these three types of cyber operations may have significant impacts on the risk of war and the outcomes of war at the strategic and tactical levels.

1. THE CURRENT STATE OF CYBER CONFLICT THEORY

It has been 20 years since the Joint Task Force - Computer Network Defense (JTF-CND) was created[1], and yet we still see a lack of a coherent Cyber Conflict Theory with adequate descriptive, predictive, and prescriptive capacities. We attribute this shortfall to the fact that the study of Cyber Conflict falls into two largely separate camps: International Relations and Information Security. International Relations experts study the phenomenon mostly using traditional conflict analysis models derived from the theory of conflict. On the

© 2021 Dr. Sergio Castro

Dr. Sergio Castro is currently the president of the Instituto de Ciberdefensa, and has 11 years of experience in information security, having worked in Microsoft, Qualys, Varonis, Elastica, Blue Coat, and Symantec. He has conducted training events and conferences on information security and cyber defense across the Americas, Europe, and Israel. He holds an M.S. in Economics, an MBA, and a PhD in Education from Universidad Abierta de San Luis Potosí, Mexico. He can be contacted at scastro@ciberdefensa.org and https://www.linkedin.com/in/castrosergio/.

other hand, Information Security experts focus on the tactical details of how cyber-attacks are conducted, but are not involved in International Relations. There have been attempts to bridge this gap, but they have been inconclusive. Applegate and Stavrou[2] developed a detailed Cyber Conflict taxonomy capable of describing in detail a cyber-attack. However, their model does not extend to the International Relations level since it cannot describe or predict the strategic or even the narrower military consequences of a cyber-attack. And this is exactly the crux of the problem: linking cyber operations to their military and broader strategic consequences.

Kello explains that "It is superfluous to state that the field of international security studies is skeptical of the existence of a cyber danger: it has barely acknowledged the issue, as reflected in the scant relevant literature."[3] Kello also states that "The costs of scholarly neglect of the cyber issue to the advancement of theory are apparent: when the range of empirical topics that theory is able to elucidate narrows, the academic enterprise inevitably enters a process of internal corrosion, which reveals itself in one or both of two ways—a loss of conceptual fertility or a reduced capacity for explanatory analysis, each of which inhibits intellectual progress in the study of international relations."[4]

We attribute this large divergence of opinion to the lack of a formal mathematical theory of Cyber Conflict. Cyber Conflict is defined as "the use of computational technologies for malevolent and destructive purposes to impact, change, or modify diplomatic or military interactions."[5] The objective of this paper is to link mathematically the use of such computational technologies with their military and broader strategic effects.

2. THE RATIONALIST EXPLANATIONS FOR WAR MODEL

Fearon published in 1995 a paper titled "The Rationalist Explanations for War."[6] In this paper, Fearon

developed a straightforward mathematical model to explain that war can be portrayed as a bargaining process. The main variables in this model are the probability of winning the war, the expected utility if the war is won, the cost it would entail for each participant, and how much we really know about these variables.

We will use this bargaining model of war as a basis to develop our Rationalist Cyber Conflict Theory, by adding information security variables that affect the model's outcomes.

2.1. THE BARGAINING MODEL OF WAR

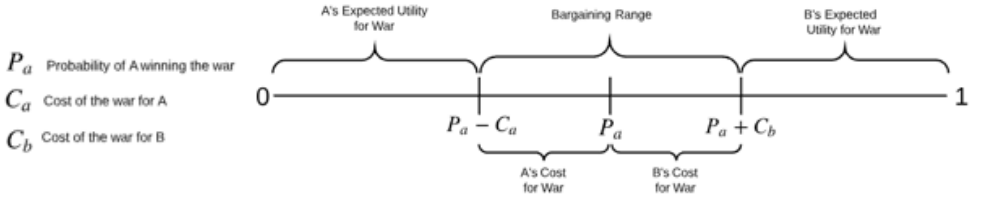


Figure 1. Baseline Model, no Cyber Operations

This is the Bargaining Model of War. Country A and country B are in conflict. We draw a line that goes from 0 to 1 to represent the value to be gained in the war; it could be territory, access to oil or minerals, etc.[7] 1 represents winning 100% of the value.

P_a represents the probability of victory for country A. Since we have normalized the possible value gain to 1, it also represents the expected utility of war. To clarify, if the total value of winning the war were $500 billion, and the probability of winning the war was 50%, then the expected utility would be Ue=$500 billion x 0.5 = $250 billion. To simplify the model, instead of using $500 billion or any other money amount, we simply use 1. Therefore, the expected utility in the model is Ue=1 x P_a, which is the same as Ue=P_a. In other words, we will be calling Pa the probability of winning the war, but it is also the normalized expected utility of winning the war.

From the utility/probability of winning the war, we need to deduct the cost of the war. This gives us P_a-C_a, which is country A's true expected utility for the war. To calculate the expected utility for country B, we take 1-P_a, and add the cost of the war for country B, C_b. This gives us the point Pa+Cb in the line. We can then see that the bargaining range goes from Pa-Ca to Pa+Cb. In other words, as long as this bargaining range exists, it makes more economic sense for country A and country B to bargain, instead of going to war. This is because if they go to war, country A can only gain Pa-Ca worth of value, whereas if it negotiates, it can gain all the way up to P_a+C_b. Same thing goes for country B. If there is a war, country B can only gain 1-(P_a+C_b), but if they negotiate, country B can gain all the way up to 1- (P_a-C_a). The likely outcome of negotiation is of course somewhere between the two end points of the bargaining range; but any outcome in this range is better than the outcomes that could be gained through war.

Therefore, if there is an x such that:

$$P_a - C_a \leq x \leq P_a + C_b$$

Then we will have a bargaining range, and war will not make economic sense.

Our thesis is that different cyber operations can modify the probability P_a, and the costs C_a, and C_b, and therefore can alter the possible outcomes of a conflict.

2.2. INFORMATION SECURITY OBJECTIVES: CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY

Information Security as a discipline has three main objectives: to ensure the confidentiality, integrity, and availability of data in the organization.

Confidentiality consists in allowing only authorized users to access data. Integrity consists in allowing only authorized users to modify data. Availability consists in ensuring that data are available to authorized users when required.

2.3. CYBER ATTACK OBJECTIVES: EXTRACTION, MODIFICATION, AND DENIAL OF SERVICE

There are three cyber offensive actions that can be taken: extraction, modification, and denial of service.

Extraction is the opposite of confidentiality: a hacker accesses confidential information and extracts it.

Modification is the opposite of integrity: the hacker modifies data without authorization, causing a disruption in the workflow supported by the IT system attacked.

Denial of Service is the opposite of availability: the hacker overwhelms an IT resource to deny its use to legitimate users.

We will call these variables the EMD variables (Extraction, Modification, and Denial of Service).

2.4. VULNERABILITIES

These actions of Extraction, Modification, and Denial of Service can be performed by hackers due to vulnerabilities in information technology systems. These vulnerabilities can be classified in three broad categories: configuration errors, technical errors, and human errors.

Configuration errors occur when IT administrators or users do not properly configure or manage IT resources. An example would be leaving a default password in a system. Since default passwords are well known, a hacker could easily access the IT resource.

Technical errors are the result of programming or hardware design mistakes. A common mistake in software programming is to mismanage memory access, giving hackers the opportunity to take over a CPU remotely by injecting malware into available memory.

Human errors occur when administrators or users do not follow proper procedures.

2.5. CYBER OPERATIONS

We propose the following taxonomy for cyber operations:

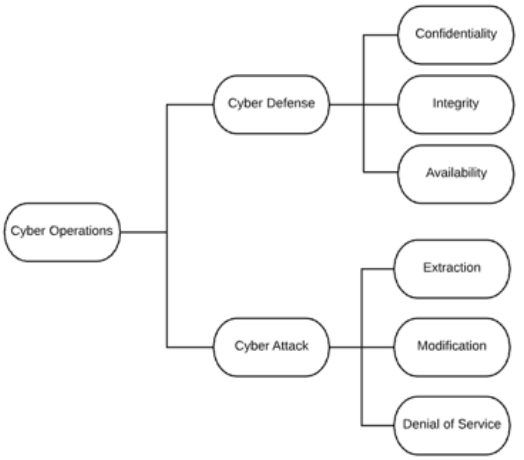


Figure 2. Cyber Operations Taxonomy

Cyber Operations are divided into action types: Cyber Defense Operations and Cyber Attack Operations. In turn, Cyber Defense, as above, is divided into three possible objectives: maintaining Confidentiality, maintaining Integrity, and maintaining Availability. Any information security software or procedure in place has to help achieve at least one of these objectives.

Cyber Attack is divided into three objectives: Extraction of data (E), Modification of data (M), and Denial of Service (D).

Cyber Operations can also be classified on their implementation level: Strategic Cyber Operations and Tactical Cyber Operations.

Strategic Cyber Operations are conducted at the nation-state level. Strategic Cyber Defense consists of the policies and plans in place to defend the infrastructure of companies and organizations within the nation-state in order to prevent strategic cyber-attacks. A Strategic cyber-attack may consist of the Extraction or Modification of valuable business, technological, or military information, or a Denial-of-Service attack that cripples vital infrastructure.

Tactical Cyber Operations are conducted during a kinetic war. Tactical Cyber Defense consists of the implementation of technical controls to prevent cyber-attacks on the command and control, communications, computer, intelligence, surveillance and reconnaissance (C4ISR) systems of a fighting force. A Tactical cyber-attack consists of the disruption of the enemy's corresponding systems through Extraction, Modification, or Denial of Service of tactical information that may affect the results of a battle.

We can combine the action types with the implementation levels into a Cyber Operations Matrix:

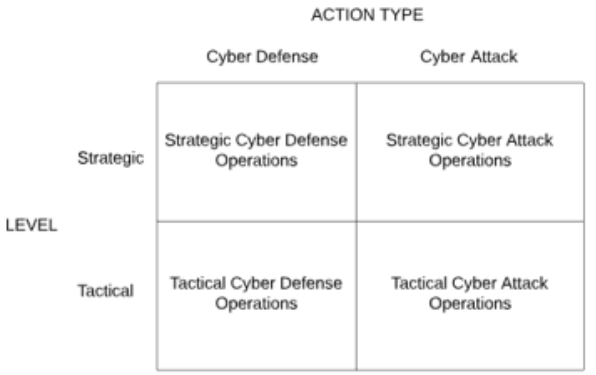


Figure 3. Cyber Operations Matrix

A nation-state must have plans in place for each of the four combinations.

The objective of Strategic Cyber Attack Operations is to disrupt the critical infrastructure of a nation-state, which can be:

- Government
- Electricity grid
- Oil and gas production and distribution
- Logistic networks
- Telecommunications
- Financial sector
- Manufacturing sector
- Services

The objective of Tactical Cyber Attack Operations is to disrupt a military unit's C4ISR systems, as well as the networks of government and civilian entities supporting a military operation. An example would be the disruption of logistical networks that feed military operations.

Both Strategic and Tactical Cyber Operations should be used as force multipliers during a kinetic war.

2.6. EFFECTS OF STRATEGIC CYBER OPERATIONS ON THE RISK OF WAR

Based on their effects on the Bargaining Model of War, we can divide cyber-attacks in the following manner:

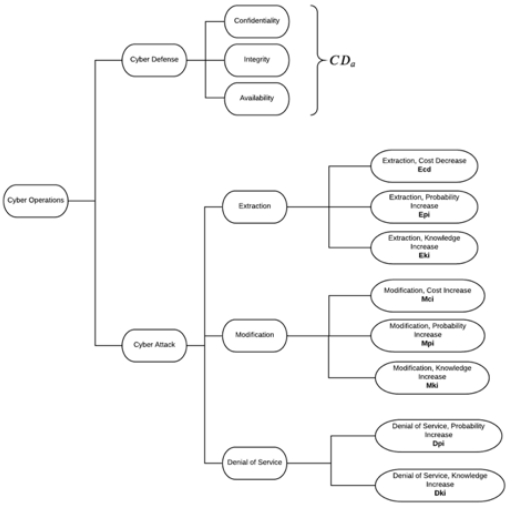


Figure 4. Cyber-attacks Taxonomy

We have divided Extraction into three types: Extraction, Cost Decrease (Ecd); Extraction, Probability Increase (Epi); and Extraction, Knowledge Increase (Eki). We are assigning them variable names because we will use them to analyze their effects in the Bargaining Model of War equation.

Modification is divided into Modification, Cost Increase (Mci); Modification, Probability Increase (Mpi); and Modification, Knowledge Increase (Mki).

Denial of Service is divided into Denial of Service, Probability Increase (Dpi), and Denial of Service, Knowledge Increase (Dki).

We saw in the Bargaining Model of War the following inequality:

$$P_a - C_a \leq x \leq P_a + C_b$$

Where P_a is the probability of country A winning the war, C_a is country A's cost of war, and C_b is country B's cost of war. Our Rationalist Cyber Conflict Theory is based on the thesis that the cyber-attack variables we listed above, Ecd, Epi, Eki, Mci, Mpi, Mki, Dpi, and Dki, have the capacity of altering P_a, C_a, and C_b, and therefore can modify the possible outcomes of a war.

Cost Decrease or Increase variables (Ecd, Mcd) can increase or decrease C_a and C_b. An Extraction, Cost Decrease (Ecd) can occur, for example, when a nation-state uses an Extraction cyber-attack to steal military technology from a rival nation-state, reducing its own research and development and production costs, part of C_a. A Modification, Cost Increase (Mci) could happen when a nation-state implements a Modification cyber-attack and sabotages the R&D or production of military technology, increasing the rival's costs, part of C_b.

Probability Increase variables (Epi, Mpi, Dpi) increase the nation-state's probability of winning the war, P_a. The nation-state can steal military technology via Extraction or can sabotage

the rival's military capacity through Modification or Denial of Service, increasing its own probability of winning.

Knowledge Increase variables (Eki, Mki, Dki) increase the nation-states' knowledge about each other's military capabilities, changing the perception of the probability of winning, P_a. In a situation in which a nation-state does not fully understand its rival's military capabilities, an Extraction cyber-attack can obtain such information, making P_a clearer. Also, a nation-state can launch a limited Denial of Service attack as a signal of its strength, increasing the knowledge of P_a for its rival. Another strategy is to do a Modification, Knowledge Increase (Mki) attack, which has been called a "flag planting attack." This consists of penetrating the rival's network and leaving evidence of the intrusion in the form of a "flag," which is a document stating that the network was penetrated, but without causing any damage. This is a clear signal of the nation-state's cyber operations capabilities and can act as a deterrent.

Regarding Cyber Defense Operations, we are adding the cost of Confidentiality, Integrity, and Availability into a single variable: CD_a.

2.7 THE RATIONALIST CYBER CONFLICT THEORY

We will now cover how the EMD variables affect the Bargaining Model of War's three variants: The Baseline Model, the Uncertainty Model, and the Preventive War Model. We will also see an example of the application of the EMD variables in game theory, used in the Preemptive War Model. We will use William Spaniel's models described in his book "Game Theory 101: The Rationality of War,"[8] and add the Extraction, Modification, and Denial of Service (EMD) variables to them, to analyze their effects on their respective bargaining ranges and probabilities of war. We will then analyze the impact of the cost of cyber defense, and finally we will examine the complete inequality of the Rationalist Cyber Conflict Theory.

2.8. BASELINE MODEL

The Baseline Model shows the simplest version of the Bargaining Model of War: country A's probability of victory is well known by both rivals, and there are no future considerations, only the present.

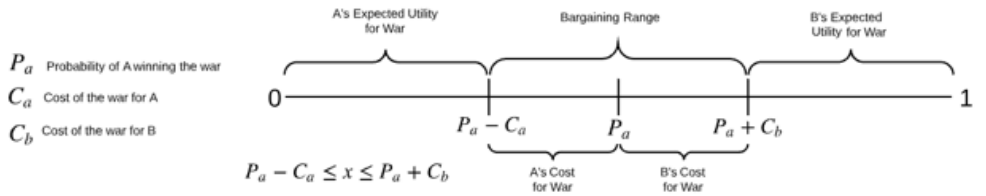


Figure 5. Baseline Model, no Cyber Operations

Above we can see the Baseline Model with no Cyber Operations. The result is that there is, theoretically, no risk of war, since there is a clear bargaining range available. This means that

the rational course of action is for both rivals to negotiate, because winning the war brings less utility (due to its cost) than any possible negotiation outcome. However, we must take into consideration that this is a model. In real life, bargaining ranges are not clearly visible, and there are emotional factors not taken into consideration by the model. But as a rule, we can say that the bigger the theoretical bargaining range and the smaller the expected utilities of war, the less probability that war will break out. A large bargaining range gives both parties more space for perception and interpretation errors, without those errors necessarily resulting in war.

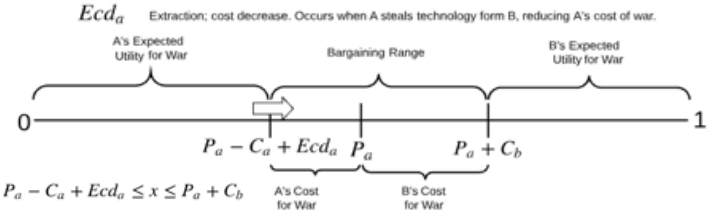


Figure 6. Baseline Model, Extraction, Cost Decrease

In this scenario, country A launches an Extraction, Cost Decrease (Ecd) cyber operation against country B. This means that country A manages to hack into country B's networks, and steals technology from country B that allows country A to conduct war in a less costly manner. This knowledge could be, for example, how to build weapons more efficiently, or knowledge on country B's military doctrine, allowing country A to plan a more efficient doctrine that requires less expensive weapons systems or troop dispositions. The end result is that country A's cost of war goes down, increasing country A's Expected Utility for War, and reducing the bargaining range. This in turn increases the risk of war; any reduction in the bargaining range has such effect because as mentioned, in real life the boundaries of the bargaining range are not clearly visible, and the smaller it is, the smaller the margin for errors in perception that could lead to war.

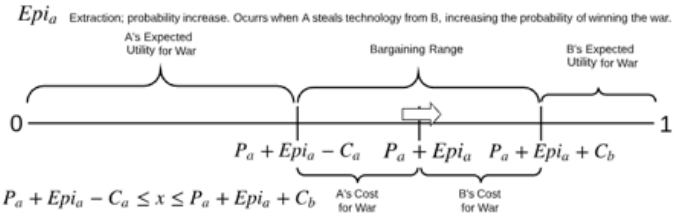


Figure 7. Baseline Model, Extraction, Probability Increase

In this scenario, country A launches an Extraction, Probability Increase (Epi) cyber operation against country B. This could be, for example, stealing technology on how to build better weapon systems, which increases the probability of winning the war. Notice that the cost does not change, only the capabilities of the weapon system. In a real-life scenario, CD_a could also increase. The result is that country A's probability of winning increases. The bargaining range

shifts in favor of country A. Also, country A's Expected Utility for War increases and country B's decreases, which in turn increases the risk that A will choose war.

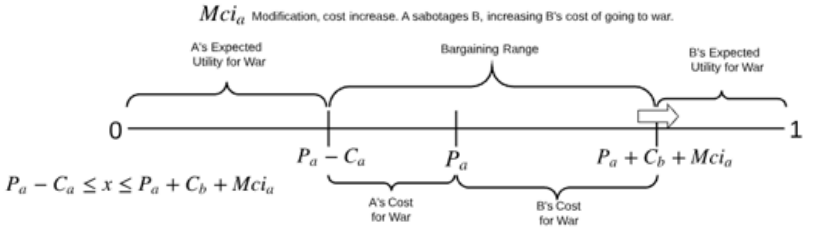


Figure 8: Baseline Model, Modification, Cost Increase

In this scenario, Country A launches a Modification, Cost Increase (Mci) against country B. This could consist of an act of sabotage that increases country B's cost of developing, manufacturing, or fielding weapons or troops. Notice that country B's probability of winning the war does not change; rather, winning becomes much costlier. Such sabotage can be intense, or it can be slow and insidious. The end result is that country B's cost of war increases. This increases the bargaining range to the advantage of A, and also reduces country B's Expected Utility for War. This reduces the overall risk of war, but significantly benefits A in the negotiations.

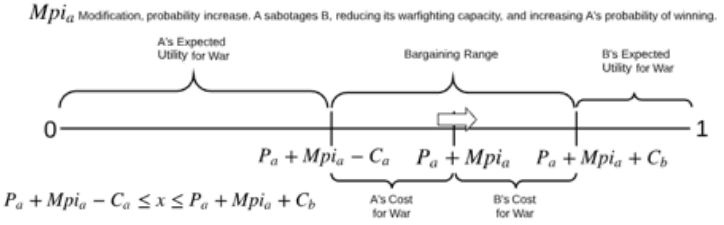


Figure 9. Baseline Model, Modification, Probability Increase

In this scenario, country A launches a Modification, Probability Increase (Mpi) cyber operation against country B. This cyber operation could consist of sabotaging country B's capacity to develop new weapons systems, thus reducing country B's probability of winning a war. The result is that country A's probability of winning the war increases. The bargaining range remains the same, but it benefits country A. At the same time, country A's Expected Utility of War increases and country B's decreases, thus increasing the overall risk of country A initiating a war if the bargaining range is not properly perceived.

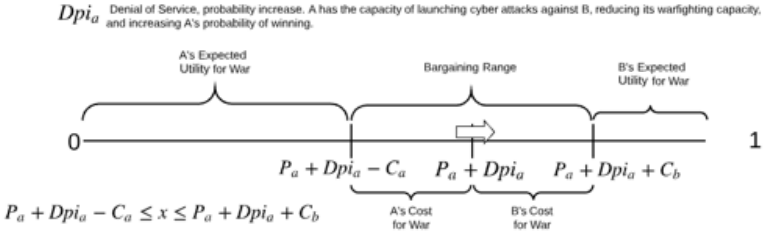


Figure 10. Baseline Model, Denial of Service, Probability Increase

In this scenario, country A launches a Denial of Service, Probability Increase (Dpi) against country B. This is a more overt version of the previous scenario, Mpi, but the end results are the same: A's probability of winning the war increases, and the bargaining range shifts in favor of country A. At the same time, country A's Expected Utility for War increases, thus increasing the risk of war.

2.9. UNCERTAINTY MODEL

The Uncertainty Model includes a more realistic complication: the disparity of perception of the probability of winning.

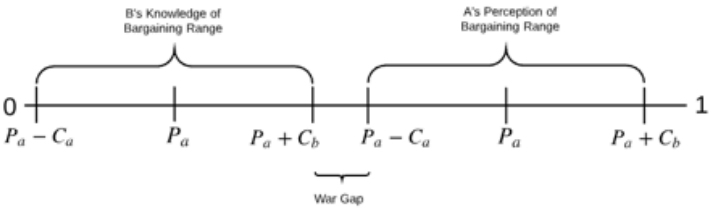


Figure 11. Uncertainty Model, no Cyber Operations

This is the Uncertainty Model, without Cyber Operations introduced yet. In this model, we assume that country B has a precise knowledge of the probability of winning, P_a, whereas country A has an erroneous perception of the probability of winning. Under this scenario, country A thinks it can win, while country B knows that the probability of country A winning is very low. We can see in the graph that there is no bargaining range, only a War Gap; therefore, it is very likely that war will occur.

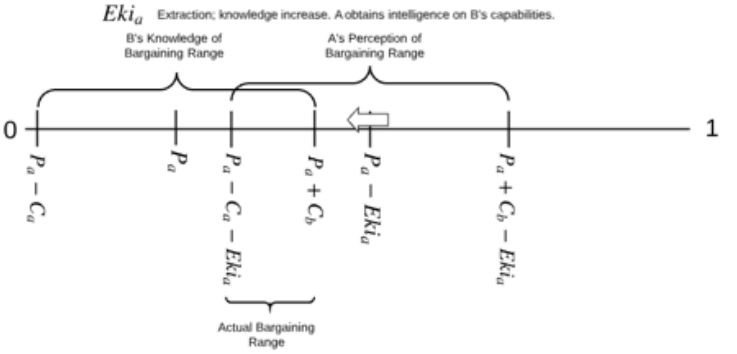


Figure 12. Uncertainty Model, Extraction, Knowledge Increase

In this scenario, country A launches an Extraction, Knowledge Increase (Eki) cyber operation against country B. This could consist of stealing information on country B's technology and troop dispositions. The result is that country A increases its knowledge on country B's capabilities, shifting country A's Perception of its probability of winning, creating an Actual bargaining range, and reducing the risk of war. In the diagram we can see that country A's perception is still not the same as country B's; however, the bargaining ranges overlap enough to make it possible for both to choose negotiation.

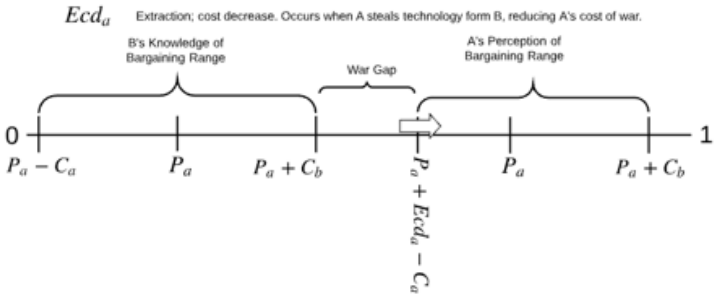


Figure 13. Uncertainty Model, Extraction, Cost Increase

In this scenario country A launches an Extraction, Cost Decrease (Ecd) cyber operation against country B. This reduces country A's cost of war, which, together with country A's wrong perception of Pa, increases the War Gap, and therefore the probability of war.

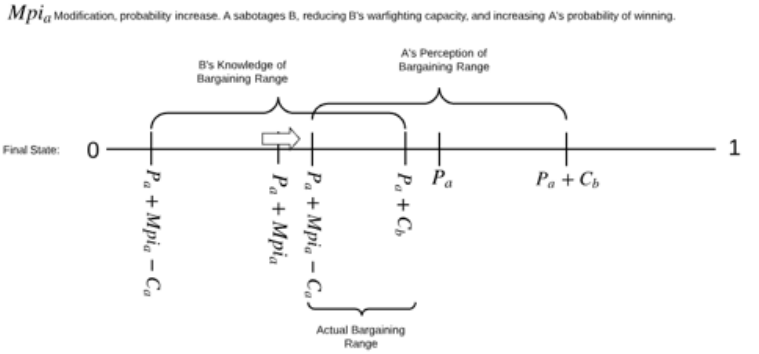


Figure 14. Cyber Operation: Modification, Probability Increase

In this scenario, country A launches a Modification, Probability Increase (Mpi) against country B, resulting in an increase in country A's probability of winning the war. If country A's perception remains the same, the actual bargaining range increases, reducing the risk of war. However, if country A's perception shifts also (not shown in the diagram), the whole equation just shifts to the right, and the chance of war does not vary.

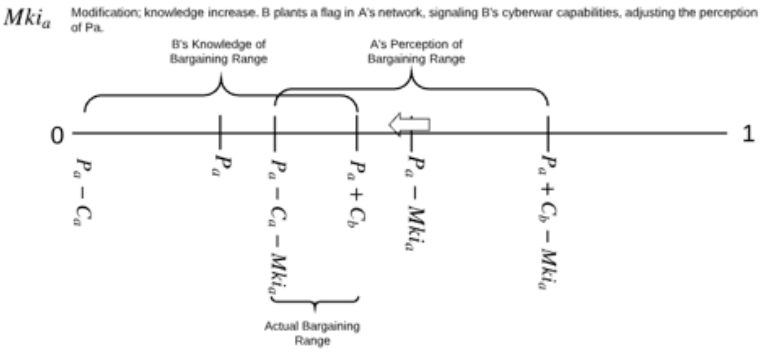


Figure 15. Uncertainty Model, Modification, Knowledge Increase

In this scenario, country B launches a Modification, Knowledge Increase (Mki) cyber operation against country A. This could consist of planting a "flag" in country A's network. A flag is an innocuous document that signals country B's capabilities of compromising country A's networks and causing damage if it so chooses. The result is that country A increases its knowledge of country B's capabilities, shifting country A's Perception of bargaining range, creating an Actual bargaining range, and reducing the risk of war.

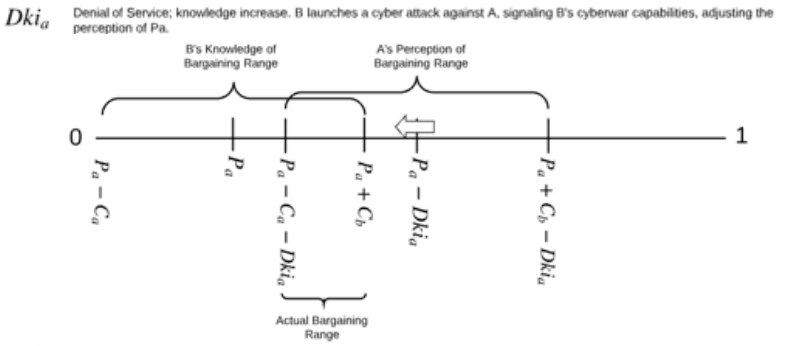


Figure 16. Uncertainty Model, Denial-of-Service, Knowledge Increase

In this scenario, country B launches a Denial-of-Service, Knowledge Increase cyber operation against country A. This is a more severe version of the previous model; country B signals its capacity and willingness to engage in cyberwar, increasing country A's knowledge of the real probability of winning, P_a. As a result, an Actual bargaining range is generated, reducing the risk of war.

2.10. PREVENTIVE WAR MODEL

We will now cover the Preventive War Model. Preventive war occurs when we have a declining state, country A, vs. a rising state, country B. Seeing the increase of power of country B, country A decides to attack before country B becomes too powerful.

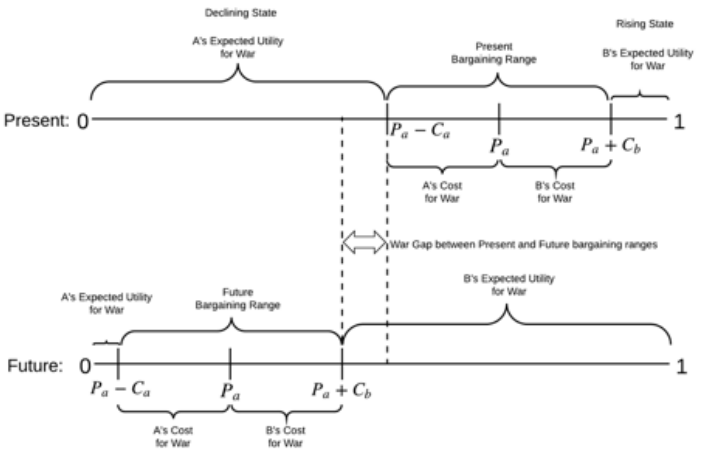


Figure 17. Preventive War Model, no Cyber Operations

This is the Preventive War Model without cyber operations. We now have two diagrams: one for the present and one for the future. In the present diagram, country A has a higher probability of winning a war, P_a, and we can see a Present bargaining range that favors country A. We can also see that in the future, since B is a rising state, country A's probability of winning a war is greatly reduced. We can see that there is a Future bargaining range, but notice how there is a War Gap between the Present and Future bargaining range. This means that country A may decide to attack country B now, before country B becomes too powerful and the probability of winning the war, P_a slides to the favor of B.

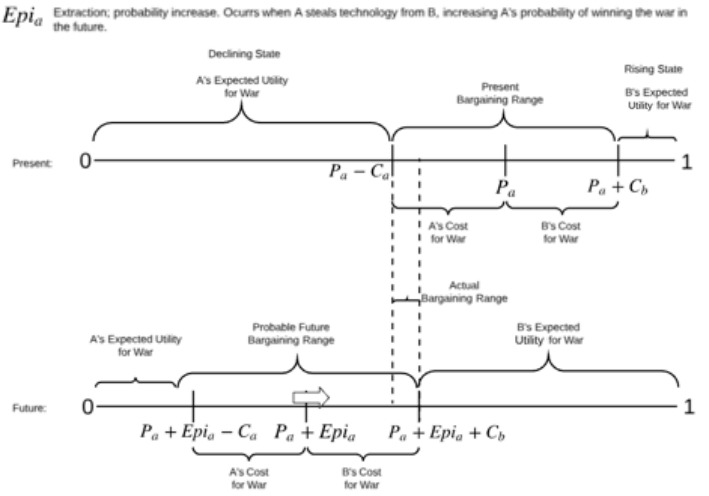


Figure 18. Cyber Operation: Extraction, Probability Increase, Declining State Steals Technology

In this scenario, country A, the declining state, launches an Extraction, Probability Increase (Epi) cyber operation, and steals technology from country B, the rising state. This increases country A's probability of winning a future war, sliding the Probable Future bargaining range to the right, in favor of country A. This creates an Actual bargaining range, reducing the risk of war.

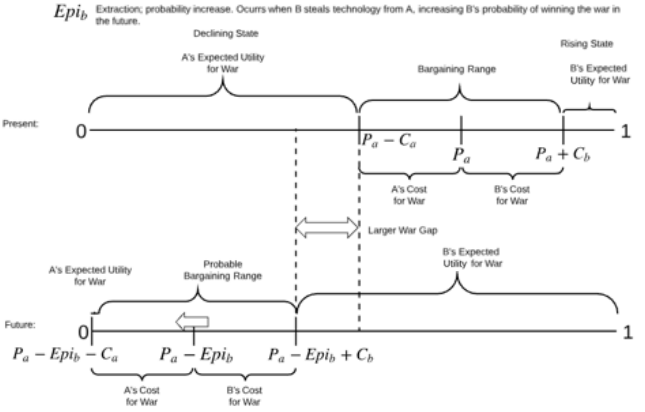


Figure 19. Cyber Operation: Extraction, Probability Increase, Rising State Steals Technology

In this scenario, country B, the rising state, launches an Extraction, Probability Increase (Epi) cyber operation and steals technology from country A, the declining state. This increases country B's probability of winning the future war, sliding the Probable bargaining range to the left, widening the War Gap, and increasing the risk of war.

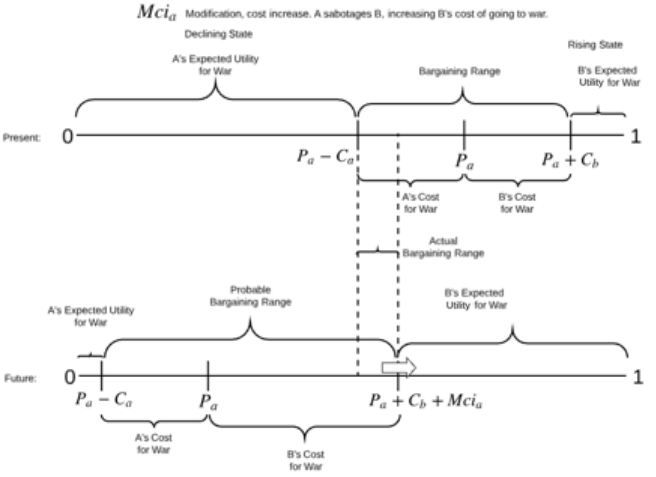


Figure 20. Cyber Operation: Modification, Cost Increase

In this scenario, country A launches a Modification, Cost Increase (Mci) cyber operation against country B, sabotaging country B's warfighting capabilities, and increasing country B's cost of war, C_b. This will increase the Probable bargaining range, creating an Actual bargaining range, and therefore reducing the risk of war.

2.11. PREEMPTIVE WAR MODEL

We will now cover the Preemptive War Model. A preemptive war occurs when country A decides to attack country B before country B attacks first, taking into consideration that the country that attacks first has a first strike advantage. For this model we will not use the Bargaining Model of War, but game theory, specifically the concept of Nash equilibrium. A Nash equilibrium occurs when the optimal outcome of a strategic interaction is one where no participant has an incentive to deviate from its chosen strategy after considering an opponent's choice.

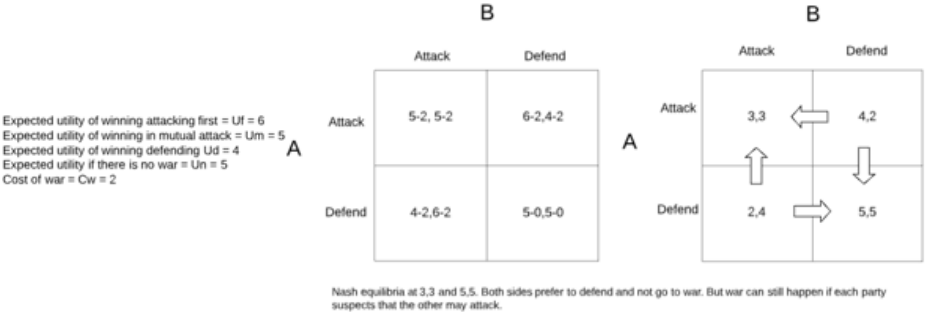


Figure 21. Preemptive War Model – No Cyber Operations

This is the Preemptive War Model without cyber operations. We will add some representative numbers to make the model work. The expected utility of winning the war when attacking first while the other side defends is 6. The expected utility of winning the war if both attack at the same time is 5. The expected utility of winning when defending is 4. The expected utility of no war, that is, both defending, is 5. And the cost of war is 2. In the first matrix of the diagram above we can use the arithmetic calculation of the total utility for each combination. For example, the total utility for both country A and country B, if they both attack, would be the expected utility of winning if both attack, 5, minus the cost of war, 2, which gives us a total utility of 3. We can see the results in the second matrix.

We can see that there are Nash equilibria at 3,3 and 5,5. Both sides prefer to defend and not go to war. The arrows show the likely movement between possible combinations. But in real life, war can still happen if there is an error of perception.

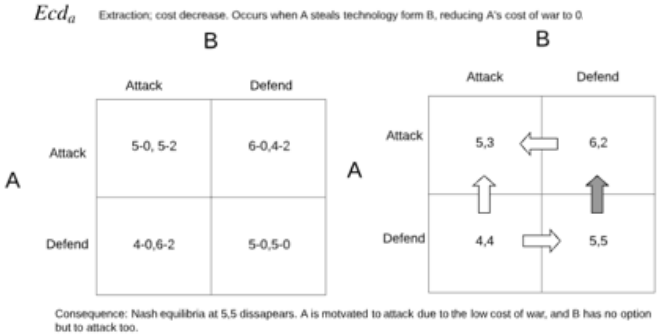


Figure 22. Cyber Operation Extraction, Cost Decrease

In this scenario, country A launches an Extraction, Cost Decrease (Ecd) cyber operation against country B, stealing technology, and reducing country A's cost of war to 0. We can see this reflected in the first matrix; instead of subtracting a cost of war of 2 to country A, we subtract 0. The result can be seen in the second matrix. The consequence is that the Nash equilibrium at 5,5 disappears, because the 6,2 combination brings more utility. At this point, country A is now motivated to attack, and country B has no option but to attack, too, to optimize its utility, leading to war. The gray arrow shows the changed flow.

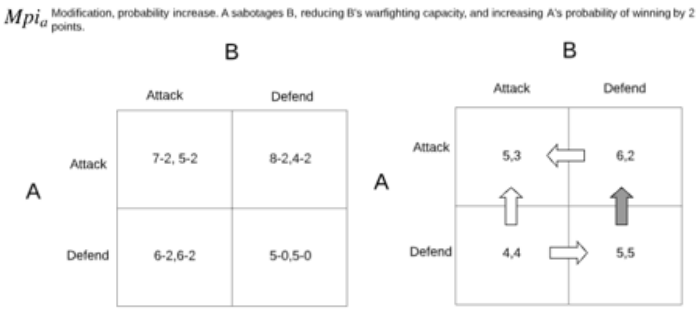


Figure 23. Cyber Operation: Modification, Probability Increase

In this scenario, country A launches a Modification, Probability Increase cyber operation against country B, reducing country B's war fighting capacity, and increasing country A's probability of winning by 2 points. The consequence is that the Nash equilibrium at 5,5 disappears, pushing the flow to 6,2, and then to 5,3, causing war.

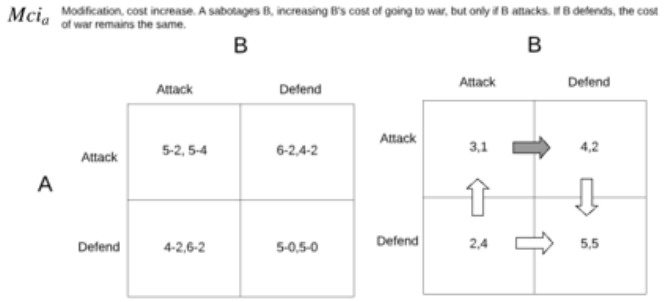


Figure 24. Cyber Operation: Modification, Cost Increase

In this scenario, country A launches a Modification, Cost Increase (Mci) cyber operation against country B, increasing country B's cost of going to war (5-4), but only if country B attacks. If country B defends, the cost of war remains the same. The consequence is that country B is not motivated to move from defend to attack, due to the reduction in utility resulting from an increase of the cost of war if it attacks. Because of this, country A is not motivated either, so they both go to defend-defend. In other words, we get a Nash equilibrium at 5,5, eliminating the risk of war.

2.12. CYBER DEFENSE IMPACT MODEL

We will now analyze the relationship between the cost of cyber defense and the probability of a cyber-attack being successful, and how this impacts the Bargaining Model of War.

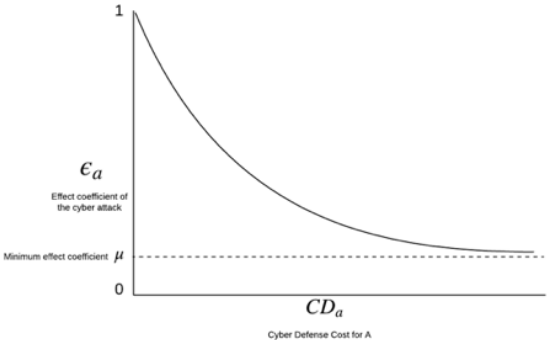


Figure 25. Cyber Defense Cost vs. Effect Coefficient

In the diagram above we can see the relationship between country A's cyber defense cost, CD_a, and ε_a (epsilon a), the effect coefficient of a cyber-attack. As we increase cyber defense spending, logically the probability of a cyber-attack being successful goes down, approaching

asymptotically a line which we call the minimum effect coefficient, μ (miu). If we invest zero in cyber defense, then the probability of being hacked is 1. As we increase our investment, the probability of being hacked approaches μ.

We now need to relate ε_a to the probability of winning the war, P_a. To do so, we multiply $1-\varepsilon_a$ times P_a, $(1-\varepsilon_a)P_a$. $1-\varepsilon_a$ describes how much the cyber-attack affects the probability of winning. For example, if we do not invest anything in cyber defense and therefore $\varepsilon_a=1$, then $1-\varepsilon_a = 1-1 = 0$, which multiplied by P_a, gives country A a zero probability of winning the war, because country B would have launched devastating cyber-attacks that render country A's military totally ineffective.

The relationship between ε_a and CD_a is expressed by the following equation:

$$\epsilon_a = \frac{1-\mu}{1+kCD_a} + \mu$$

Where k is a constant that shapes the curve. If the investment in cyber defense, CD_a, is equal to zero, then $\varepsilon_a=1$, meaning that the probability of getting hacked is 100%.

If we substitute this equation into $(1-\varepsilon_a)P_a$, we get the following:

$$\left(1 - \frac{1-\mu}{1+kCD_a} + \mu\right) P_a$$

This part of the equation is telling us that as we increase our cyber defense expenditure, CD_a, the probability of a cyber-attack being successful goes down to a minimum of μ, and therefore the probability of winning the war, P_a, goes up from 0 (when $\varepsilon_a = 1$) and approaches P_a (1- μ) (when CD_a is very large).

When we insert this into the overall equation, and also subtract CD_a since it's also part of the cost of war, we get the following inequality:

$$\left(1 - \frac{1-\mu}{1+kCD_a} + \mu\right) P_a - C_a - CD_a \leq x \leq \left(1 - \frac{1-\mu}{1+kCD_a} + \mu\right) P_a + C_b$$

Let us see how this equation affects the Bargaining Model of War.

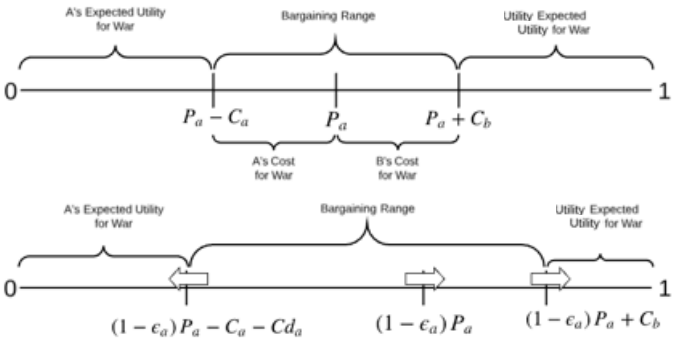


Figure 26. Baseline Model, No Cyber Operations & Implement Cyber Defense

On the previous page we can see the Baseline Model with no cyber operations, and the Baseline Model with cyber defense implemented. We can see that as CD_a increases, the probability of winning for country A, P_a, increases. This happens because, as we saw, as CD_a increases, the effect coefficient of a cyber-attack, ε_a, decreases, and therefore P_a increases. This increase in Pa shifts the bargaining range to the right, favoring country A. At the same time, the increase in CD_a expands the bargaining range to the left, reducing country A's Expected Utility for War. So, in general, increasing CD_a reduces the risk of war, shifting the bargaining range to country A's benefit.

2.13. COMPLETE INEQUALITY

Here we can see the complete inequality for the Rationalist Cyber Conflict Theory.

P_a	Probability of A winning the war
C_a	Cost of the war for A
C_b	Cost of the war for B
Ecd_a	Extraction; cost decrease. Occurs when A steals technology form B, reducing A's cost of war.
Epi_a	Extraction; probability increase. Ocurrs when A steals technology from B, increasing the probability of winning the war.
Eki_a	Extraction; knowledge increase. A obtains intelligence on B's capabilities.
Mci_a	Modification, cost increase. A sabotages B, increasing B's cost of going to war.
Mpi_a	Modification, probability increase. A sabotages B, reducing its warfighting capacity, and increasing A's probability of winning.
Mki_a	Modification; knowledge increase. A plants a flag in B's network, signaling A's cyberwar capabilities, adjusting the perception of Pa.
Dpi_a	Denial of Service, probability increase. A has the capacity of launching cyber attacks against B, reducing its warfighting capacity, and increasing A's probability of winning.
Dki_a	Denial of Service; knowledge increase. A launches a cyber attack against B, signaling A's cyberwar capabilities, adjusting the perception of Pa.
T	The sum of the required combination of Ecd, Epi, Eki, Mci, Mpi, Miki, Dpi, and Dki.
CD_a	Cyber defense cost for A
μ	Minimum effect coefficient
k	Cyber defense curve constant

$$\left(\frac{1-\mu}{1+kCD_a}+\mu\right)P_a - C_a - CD_a + T \leq x \leq \left(\frac{1-\mu}{1+kCD_a}+\mu\right)P_a + C_b + T$$

3. MODEL PREDICTIONS

The Rationalist Cyber Conflict Theory is a theoretical model, not an empirical one. This means that it is not designed to make precise predictions, but rather to aid in understanding of possible cause-and-effect dynamics.

1. Strategic Cyber Operations in the form of Extraction, Modification, and Denial of Service, have the capacity of modifying the probability of winning a war, and the cost of a war.
2. In the Bargaining Model for War, the larger the bargaining range is, the less likely it is that there will be a war.
3. A cyber operation that increases the cost of war (Mci) increases the bargaining range, and therefore reduces the risk of war. In other words, the costlier the war, the less likely it will happen.
4. A cyber operation that decreases the cost of war (Ecd) reduces the bargaining range, and therefore increases the risk of war.

5. A cyber operation that increases the probability of winning a war (Epi, Mpi, Dpi) does not modify the magnitude of the bargaining range, but it does shift it in favor of country A. This also means that country A's Expected Utility for War increases. If the bargaining range is small and country A's Expected Utility for War is large, there is a greater probability that country A may misjudge the situation and cause a war.
6. A cyber operation that increases knowledge (Eki, Mki, Dki) causes the convergence between country A's and country B's perception of the probability of winning the war, making the bargaining range more visible, and reducing the risk of war.
7. In a preventive war scenario, if a rising state launches cyber operations that increase its future probability of winning the war (Epi, Mpi, Dpi), it will increase the War Gap between the present and future bargaining ranges, increasing the risk of war. The faster a rising state steals technology from the declining state, the higher the risk for war.
8. If a declining state launches cyber operations that increase its future probability of winning the war (Epi, Mpi, Dpi) by stealing technology from the rising state, it will create an actual bargaining range, reducing the risk of war.
9. In a Preemptive War Model, modeled with game theory, any cyber operation that increases the probability of winning the war, will increase the probability of war; any cyber operation that increases the cost of war reduces the risk of war; and any cyber operation that decreases the cost of war increases the risk of war.
10. An increase of cyber defense spending will increase the probability of winning a war but will also increase the cost of war. This will cause a shift of the bargaining range in the favor of country A, and increase the size of the bargaining range, reducing the risk of war.
11. Every cyber operation, when discovered, becomes a Knowledge Increase operation in a sense, because country B learns about country A's cyber operations capabilities.

It is important to note that the model focuses on cyber operations undertaken by nation-states with clear geopolitical goals in mind. The model does not cover cybercrime activities, hacktivism, cyber terrorism, or emotion-driven attacks from cyber militias outside the control of the nation-state.

4. CONCLUSION: IMPLICATIONS OF THE MODEL FOR CYBER WARFARE DOCTRINE

The objective of a national cyber doctrine is to describe the procedures that will be put into place to achieve specific objectives against rivals in the cyber domain. We offer here some strategy and policy implications drawn from the modeling; these ideas need also to be considered in their broader strategic and security contexts.

Cyber doctrine should be organized according to this Cyber Operations Matrix:

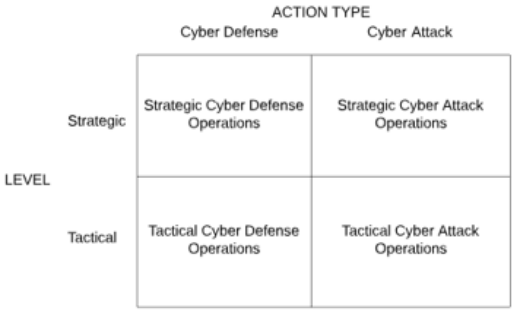


Figure 27. Cyber Operations Matrix

The first consideration is that the entities that implement each of the four quadrants should be independent from one another, albeit with close coordination.

All Cyber Attack Operations should be conducted by the armed forces or other governmental entities explicitly operating under the authority of the nation's defense leadership, given the possible political and military implications of such attacks. Allowing independent civilian organizations to participate in such cyber operations, such as hack-backs, could easily get out of hand. Likewise, Tactical Cyber Defense Operations should logically be conducted by the armed forces, given the fact that the networks being defended are military.

On the other hand, Strategic Cyber Defense Operations should be a coordinated effort of civilian entities and the armed forces. The logic behind this is that many of these types of cyber operations happen mainly in civilian networks.

We will now cover in detail the implications of the model for Strategic Cyber Defense Operations, Strategic Cyber Attack Operations, and Tactical Cyber Operations.

4.1. IMPLICATIONS FOR STRATEGIC CYBER DEFENSE OPERATIONS

Companies tend to invest in information security no more than the expected loss that could result from a hack, expressed by the probability of being hacked times the loss of a breach. This is an optimum behavior for a single company, but very much suboptimal for the entire nation-state. For example, if a telecom gets hacked as a prelude to a kinetic war, the telecom loses money, but also the entire nation-state becomes vulnerable due to the lack of telecommunications when the war starts.

We can describe this investment dynamic with the following graph:

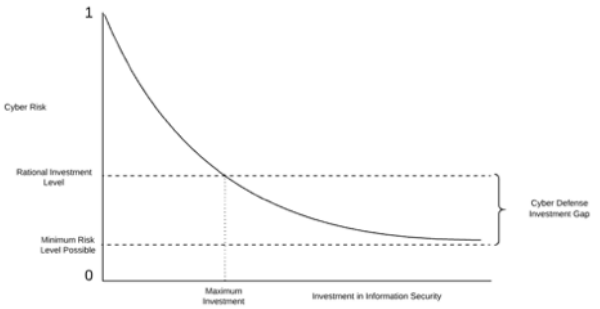


Figure 28. Rational Investment Level

As we increase investment in information security, cyber risk goes down. In theory, if we were to invest enough, we would approach asymptotically the Minimum Risk Level Possible line. However, companies will stop at the Rational Investment Level, which is equal to or less than the expected loss of a hack. This will generate a Cyber Defense Investment Gap like that shown on the graph, which represents a danger for the nation-state. The only way of reducing this gap is through government action that would reduce the cost of information security for companies. For example, the government could subsidize software, equipment, and training in information security for strategic infrastructure companies, or it could give special tax breaks on their purchase. This economic support would shift the Rational Investment Level down, reducing the Cyber Defense Investment Gap.

A related problem is the jobs gap for information security professionals. According to the 2017 Global Information Workforce Study,[9] the worldwide information security workforce gap will reach 1.8 million by 2022. We put forth that the reason behind this shortage is rooted in the Rational Investment Level. The jobs market is ruled by the forces of supply and demand, and the price that responds to differences between supply and demand for a job type is its salary. Given the large supply-demand gap in information security jobs, the salaries for such positions should be extremely high. If they were, this salary signal would eventually attract enough information security professionals to fulfill those jobs. But there is an economic restriction: The Rational Investment Level. Infosec salaries are a large component of a company's annual information security expenses, and a company will not invest above its Rational Investment Level, which is equal to or lower than the expected loss of being hacked, calculated by multiplying the risk of being hacked in a given year times the cost of a breach. So, no matter how large the information security gap is, salaries are not going high enough to close the gap thanks to this investment limit. We believe that the only possible solution is for governments to subsidize the training and salaries of information security professionals, remembering that this not only benefits the companies, but increases the national security of the country.

On the other hand, as a response to the lack of enough qualified cybersecurity professionals, information security vendors are developing automated solutions driven by AI. We can expect this trend to grow, and eventually reach a point in which most cyber defense and cyber-attack processes will be largely executed by AI.

4.2. IMPLICATIONS FOR STRATEGIC CYBER ATTACK OPERATIONS

A nation-state may choose as part of its cyber doctrine not to engage in Cyber Attack Operations and focus only on cyber defense; that is a rational option if the nation-state does not have other nation-states as natural enemies.

For those nation-states that do have rivals and wish to engage them in the cyber domain, the main implication of this model starts with the concept that they only have three general types of strategic Cyber Attack Operations they can engage in (Extraction, Modification, and Denial-of-Service), and that these cyber operations should be used to achieve strategic shifts in relations with geopolitical rivals. Therefore, the nation's cyber security community should develop a catalog of possible Extraction, Modification, and Denial-of-Service actions it could implement against each rival's economic, political, and military programs, to achieve specific strategic or military objectives. These plans should include an analysis indicating how each operation may increase or decrease the probability of winning a war, how it may increase or decrease the costs, and how it may modify the bargaining ranges. Logically, the cyber security community should also analyze the possible Extraction, Modification, and Denial-of-Service cyber operations that rivals could launch against their nation-state, what would be the strategic motivations and consequences, and which Cyber Defense Operations should be in place to neutralize these strategic cyber-attacks.

It is important to note that Extraction and Modification can be conducted equally during peacetime and wartime, whereas Denial-of-Service should be used almost exclusively during wartime. This is because Denial of Service attacks can be temporarily devastating, but countries have the capacity to recover quickly from them. Therefore, it makes little sense to launch a Denial-of-Service attack if it is not going to be followed by a kinetic war, since such an attack would achieve nothing. The only exception to this is a Denial-of-Service, Knowledge Increase (Dki) attack, used to signal the nation-state's cyber-attack capabilities. But one must take into consideration that after each attack, the rival will learn from it and harden its defenses. The best use of a Denial-of-Service attack is to launch it as a prelude to a kinetic war, to throw into disarray the enemy's electrical grid, telecom services, logistics, and financial services, and use that as a force multiplier for the kinetic war that would follow immediately. Using a street fight as an analogy, the Denial-of-Service attack is the equivalent of knocking your opponent to the ground, while the kinetic war attack is the equivalent of pounding on him once he's on the floor. If you just knock him to the ground and stop at that, he will just get up.

4.3. IMPLICATIONS FOR TACTICAL CYBER OPERATIONS

In their paper "Understanding Centers of Gravity and Critical Vulnerabilities,"[10] Strange and Iron postulate that a center of gravity has three characteristics: critical capabilities, critical requirements, and critical vulnerabilities. Within the context of a military unit, its critical capabilities are the means it has to fulfill its operational mission. Its critical requirements are the conditions and resources essential for the military unit to exercise its critical capabilities. And its critical vulnerabilities are those critical requirements that can be neutralized by the enemy, significantly reducing the military unit's critical capabilities. As an example, a critical capability of a battalion is the firepower it can bring to bear against enemy forces. Its critical requirements are personnel, equipment, fuel, ammunition, supplies, etc. Its critical vulnerabilities are the core requirements that can be attacked by the enemy under its current operational scenario; these could be, for example, supply lines, or telecommunication capabilities through an electronic warfare attack.

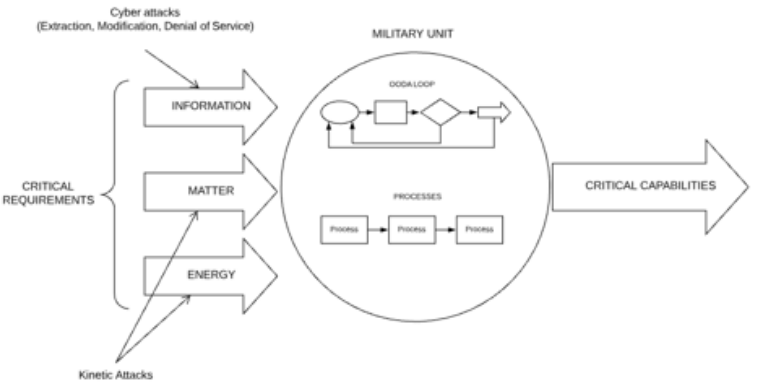


Figure 29. Center of Gravity

In this Critical Requirements and Critical Capabilities diagram we see that we can further deliver critical requirements into three categories: information, matter, and energy. Matter critical requirements can be equipment and ammo, for example. Energy critical requirements are fundamentally fuel and electricity. And information critical requirements are the capabilities provided by C4ISR systems (command, control, communications, computer, intelligence, surveillance and reconnaissance). Within the military unit, we can see the OODA Loop (observe–orient–decide–act), which is the method used to process all information coming into the unit and decide how to respond. We can also see that there are other processes running that are not related to decision making but are important for the unit. When all the critical requirements are met, and the OODA Loop and support processes are running correctly, then the military unit can deliver its critical capabilities. On the other hand, an attack on its critical requirements will degrade its critical capabilities.

Matter and energy requirements are affected through kinetic attacks, such as attacking supply lines and bombarding supply depots. And germane to the model, information requirements are affected through tactical cyber-attacks, in the form of Extraction, Modification, and Denial of Service (EMD) operations launched against C4ISR systems. Military planners should focus on identifying the information security vulnerabilities that, when attacked, would cause the most degradation to the OODA Loop of the enemy military unit. Likewise, they should identify the vulnerabilities within the information critical requirements of their own military units, and how to protect them.

It is important to note that the EMD cyber operations can be either intensive and close to the battlefield, or insidious and far removed from the battlefield. An intensive attack could be a Denial of Service of a system controlling military telecommunications. While effective, such an attack is immediately obvious, and the enemy will likely be able to mitigate it in some way. On the other hand, an insidious attack could be, for example, the modification of a database in an equipment maintenance warehouse that causes the system to order the wrong parts for critical equipment. By the time the enemy discovers the attack, its critical capabilities may be significantly diminished, and it will take a long time to recover. So, both intensive and insidious EMD tactical cyber operations should be combined for maximum effect. The critical point is that military planners should make the maximum effort to identify and understand the systems and procedures of the enemy's military units, develop a catalog of possible EMD attacks and their effects, and plan for the syncing of cyber-attacks with kinetic attacks to achieve a force multiplier effect. Likewise, they should map to the maximum detail possible the systems and procedures of their own military units, identify their information critical requirements, pinpoint their vulnerabilities, and implement the required tactical cyber defense systems.

NOTES

1. US Cyber Command History, (n.d.), Retrieved from https://www.cybercom.mil/About/History/.
2. S. D. Applegate & A. Stavrou, (2013, July 25), Towards a Cyber Conflict Taxonomy. In *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, https://ieeexplore.ieee.org/document/6568391.
3. L. Kello, (2013), The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security*,38(2), 7-40. doi:10.1162/isec_a_00138.
4. Ibidem.
5. B. Valeriano and R. C. Maness, (2015), *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (New York: Oxford University Press).
6. J. D. Fearon, (1995), Rationalist explanations for war. *International Organization*,49(03), 379. doi:10.1017/s0020818300033324.
7. W. Spaniel, (2012), *Game theory 101: The rationality of war*. Createspace.
8. Ibidem.
9. The 2017 Global Information Security Workforce Study, (2017). Retrieved from https://iamcybersafe.org/wp-content/uploads/2017/06/europe-gisws-report.pdf.
10. Dr. J. Strange & Colonel R. Iron (n.d.), Understanding Centers of Gravity and Critical Vulnerabilities. Retrieved from http://www.au.af.mil/au/awc/awcgate/usmc/cog2.pdf.

Microtargeting as Information Warfare

Jessica Dawson, Ph.D.

ABSTRACT

Foreign influence operations are an acknowledged threat to national security. Less understood is the data that enables that influence. This article argues that governments must recognize microtargeting—data informed individualized targeted advertising—and the current advertising economy as enabling and profiting from foreign and domestic information warfare being waged on its citizens. The Department of Defense must place greater emphasis on defending servicemembers' digital privacy as a national security risk. Without the ability to defend this vulnerable attack space, our adversaries will continue to target it for exploitation.

INTRODUCTION

In September 2020, General Paul Nakasone, NSA Director and Commander of U.S. Cyber Command, called foreign influence operations "the next great disruptor."[1] Nearly every intelligence agency in the United States government has been sounding the alarm over targeted influence operations enabled by social media companies since at least 2016, even though some of these operations started earlier. What often goes unstated and even less understood is the digital surveillance economy underlying these platforms and how this economic structure of trading free access for data collection about individuals' lives poses a national security threat. Harvard sociologist Shoshana Zuboff calls this phenomenon "surveillance capitalism [which] unilaterally claims human experience as free raw material for translation into behavioral data."[2] This behavioral data is transformed into increasingly accurate micro-targeted advertising.[3] The new surveillance capitalism has enabled massive information warfare campaigns that can be aimed directly at target populations. The predictive power of surveillance capitalism is not only being leveraged for advertising success but increasingly harnessed for mass population control[4] enabled by massive amounts of individually identifiable, commercially available data with virtually no oversight or regulation.

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

Jessica Dawson is an Assistant Professor and Research Scientist at the Army Cyber Institute. She holds a Ph.D. in sociology from Duke University and her research is focused on the intersection of social cohesion, narratives, and technology.

This is not to say there is no oversight—data use and collection by the intelligence community is subject to significant oversight and regulation. This article, critically, is not about data use laws and areas that are already regulated. Technology companies such as Facebook or Google exist in ungoverned spaces and are not subject to regulations like specific industries such as banking, education, or health care providers. For example, medical companies are clearly bound by Health Insurance Portability and Accountability Act (HIPAA) and the banking industry is bound by Sarbanes Oxley, which includes data regulation components. Conversely, the tech companies actually have a shield from liability based on the Communications Decency Act, Section 230.[5] This law places tech companies outside of regulatory restrictions rather than providing any meaningful limit on their actions and as a result creates a national security risk for the Department of Defense (DoD).

For example, Facebook has acknowledged its platforms'[1] abilities to help political campaigns target voters to defeat ballot initiatives[6] and, more recently, Channel 4 News in the United Kingdom reported on how political action committees (PACs) in the US targeted voters to decrease opposition turnout using the Cambridge Analytica dataset.[7] These incidents, and others have caused people to look at the concentrated power companies leveraged via these platforms. This article argues microtargeting allows individual-level messaging to be deployed to influence voting behavior and is able to be leveraged for more insidious dis/misinformation campaigns. What started as a way for businesses to connect directly with potential customers has transformed into a disinformation machine at a scale that autocratic governments of the past could only imagine. The US must recognize the current advertising economy as enabling and profiting from information warfare being waged on its citizens and address the threat.

[1] Facebook also owns Instagram, Oculus, and WhatsApp.

Fundamentally, domestic digital privacy is a national security issue. The DoD should place greater emphasis on defending servicemembers' digital privacy as a national security threat. This is not a hypothetical issue. China recently accused a staff sergeant of being patient zero in the COVID-19 pandemic, which unleashed a torrent of attacks online against her.[8] Targeting of key individuals by foreign agents has always been a national security threat, and yet the current advertising ecosystem is not currently widely recognized as an attack space. Consider a defense contractor that targets a senior military leader in order to sway his/her decision on an acquisition. What if a missile systems operator is identified and targeted for digital blackmail by North Koreans? Worse, consider if China is successful in convincing key US military officers that it poses no threat in the Pacific, leading to changes in the force posture that work in China's benefit. The murder of a Mexican American soldier and subsequent social media outrage at Fort Hood in 2020 demonstrates the impact a local incident can have on the national scale. All of this is enabled, with surgical precision, by the microtargeting advertising environment, fed by data gathered through apps, cell phones, games, and more.

UNDERSTANDING DATA

Everyone who has ever bought a car or house, or applied for a credit card, understands that companies gather data about you, the consumer. An individual's credit report shows what accounts they have, and the balances owed, and helps lenders determine if an individual is at high risk (low credit score) or low risk (high credit score) of paying back the loan. In a way, this is quantified trust. Credit reports are also auditable—every American is entitled to free credit reports each year to ensure that no one has opened accounts in their name or to ensure that nothing on the report is erroneous.

Expanding further, companies such as Mastercard know everything an individual has purchased on their credit card. Amazon knows what you have purchased on Amazon as well as how you paid for it. Companies have been gathering data on their customers for years, but the key element is that Mastercard knows one piece of this information, Amazon another, and so on. They do not know how you voted, for example, nor should they include that information in whether you get approved for a credit card. All of this changed as data became more ubiquitous and storage became cheaper.

In the early days of the Internet, advertising paved the way to support platforms' ability to be "free" —in exchange for access, customers gave up certain data. In turn, these companies used the data to better target advertising to potential buyers. First Google, then Facebook, figured out how to monetize all the information on individuals. Facebook quickly realized how much information it had on individuals and how much it could continually gather. Other data brokers, such as Experian, Axiom, Magellan, and others, "followed people throughout their digital lives, through every move and every purchase, collecting as much as possible in order, ostensibly, to provide credit scores but also to make a profit in selling that information."[9] Despite

initial outrages over privacy invasion, it became second nature to expect everything for free or low-cost subscriptions—music in terms of apps like Pandora, Spotify, or YouTube in terms of free music videos, tv shows etc., or Tiktok, allegedly the last happy place on the Internet. All this entertainment was accessed for free—or was it? The old adage that if you are not paying for a product you are the product is not entirely true. Not only are we the product but every aspect of our daily lives provides the raw material for this entire economic model. Companies are making billions of dollars off everyday life events with functionally no oversight, no regulation, and no meaningful ability to opt out.[10]

ADVERTISING THEN AND NOW

There is an old quote in advertising that about 50% of it works, but advertisers don't know which 50%.[11] Advertising has always been only "one small piece of getting consumers to buy"[12] and exists within a larger cultural framework. The holy grail of advertising has always been "bring a particular message to a particular moment to have a high probability of influencing their behavior."[13] That desired behavior change has typically been targeted toward purchasing a product, and "mass behavior medication techniques [were defined as] unacceptable threats to individual autonomy and the democratic order."[14] This instrumentarian power has been justified as unavoidable and inevitable in the pursuit of more targeted advertising. Yet, only once the power of this data began being used for political purposes did governments and people slowly begin to realize the level of influence a few private companies exert over their perception. Over the last 20 years, new "more complex means of behavior modification" have emerged along with a new, logic-based "instrumentarian power [which] knows and shapes human behavior towards other's ends."[15] While culture is a highly contested concept, for this article, it will be defined as "an attention-focusing institution."[16] Social media design has been focused on capturing and selling access to that attention by better targeting content to keep people engaged.[17] Political advertising has benefited tremendously from this new, highly detailed information about potential voters.

Social science research typically uses demographic groups such as race, gender, and political affiliations to identify social groups' patterns and trends. For example, the 1980 election was the first time there was a significant gender gap between women and men voters in support for President Reagan.[18] Prior to surveillance capitalism enabling targeted advertising, political advertising was similar to other social science research. People were broken into large categories using variables that served as proxies for meaningful behavior.[19] Women were more likely to vote for education and healthcare than men, who were more likely to be motivated by national defense issues and the economy. Republicans were motivated by different issues than Democrats.[20] However, these categories have historically been large and imprecise, which meant messaging had to be broad, and, as a result, broad messages would not necessarily resonate with the intended audience.

In order to understand why the transition to surveillance capitalism has enabled a new form of information warfare, we must first understand microtargeting as enabled by algorithms. These algorithms—computer code that shapes outcomes and records the responses—should be understood as "products of social forces."[21] These algorithms did not always reflect such detailed knowledge about individual users; however, as more and more users "shared" more and more details about their lives, Facebook realized it had tremendous pools of new data from which to glean—and monetize—insights. "When people signed on to play games such as Candy Crush on Facebook, and clicked "yes" to the terms of service for that third-party app, they were opting in to give their data and the data of all their friends, for free, to the app developers and then, inadvertently, to everyone with whom that app developer had decided to share the information."[22]

Data-driven insights could be used to better target advertising in more and more effective ways. In his book *Mindf*ck*, Cambridge Analytica whistleblower Chris Wylie describes discovering suburban women who do yoga, shop at Whole Foods, and yet attend anti-LGBTQ churches and donate to anti-gay causes.[23] Messages targeted to a voter in this demographic would have to be wholly different than messages targeted toward women who match those same demographic characteristics but do not attend anti-LGBTQ churches. A Facebook employee was stunned to discover that advertisements for TikTok that looked like they would be better targeted toward teen girls were in fact accurately targeted toward his demographic: middle aged men were being targeted with videos of teen girls dancing. The accuracy of these algorithms is still being investigated by researchers but evidence suggests that "based on only sixty-eight Facebook 'likes' an individual user might have garnered...those few 'likes' [could] predict skin color, sexual orientation, political party affiliation, drug and alcohol use, and even whether a person had come from an intact or a divorced household."[24] Data-enhanced modeling is arguably more accurate than human assessments.[25] The more data available to these companies, the greater accuracy that these messages can be targeted to drive desired behavior. There is a saying that "Google knows you better than your mother" because it has access to nearly every aspect of an individual's online activity from appointments, to meetings to photos and searches, which may be highly embarrassing if they were ever to become public.[26] The Facebook newsfeed is not displaying articles and updates in chronological order—users are seeing content that is continually tested to capture more of the user's attention and spark emotional response.[27]

FROM MICROTARGETING POLITICAL MESSAGES TO SOCIAL CONTROL

As early as 2011, the Defense Advanced Research Projects Agency (DARPA) researched social media information-sharing patterns and social media psychological profiling.[28] Combining demographic information with psychological profile information like the Big Five Personality test apparently increased the accuracy of voting messaging.[29] The Big Five Personality trait test measures people along five-axes: openness, agreeableness, conscientiousness, neuroticism,

and excitableness.[30] For example, according to Cambridge Analytica's research, Republicans tend to rate higher on conscientiousness than Democrats. The 2008 Obama campaign was one of the first to purchase additional data such as magazine subscriptions and automobile buying history to provide "more context to each voter…yielding far more accurate information."[31] The possibilities for using this detailed information to inform political messaging were realized early on by the Obama campaign, which was the first to use the term "persuadables" in attempting to quantify how likely some voters were to be persuaded to cast their vote for Obama.[32] A key aspect of these efforts is a form of experimentation known as A/B testing to find the right content to elicit the desired response.

Following the 2016 presidential election, people became aware of the scale and detail associated with microtargeting political campaigns. As a result, Cambridge Analytica became one of the most notorious examples of data-assisted political microtargeting. It took traditional voter research and aggregated it with unprecedented levels of data. Cambridge Analytica developed an app called "My Personality…to build the first precise models of millions of Facebook users."[33] It combined census data with political affiliation with shopping preferences. From Experian, it purchased "airline memberships, media companies, charities, amusement park attendances as well as government licenses."[34] Combing all of this along with social media information, church attendance behavior, personality information, and voter polling provided a level of detailed analysis on individuals broken down by voting district.[35] By framing messaging according to "psychometric profiles," behavior modification can be achieved more reliably. "Persuasive appeals that were matched to people's extraversion or openness to experience level resulted in up to 40% more clicks and up to 50% more purchases than their mismatching or un-personalized counterparts."[36] Some of the marketing material claimed to have up to 750 data points per person. The company also used traditional social science research methods like focus groups to determine what issues on the ground people cared about rather than relying on representative surveys. This gave its analysts powerful underlying knowledge of their target audiences. For example, the slogan "Drain the Swamp" rose out of focus groups conducted two years before the 2016 election.[37]

Beyond domestic political campaigns, governments like the People's Republic of China are using data-driven analytics to exert social control over their own population. Over 1 billion Chinese users conduct over 60% of their transactions through the app WeChat,[38] giving the Chinese Communist Party (CCP) data not only about what people are buying but also the opportunity to deny people the ability to make purchases. WeChat "is state-recognized, electronic social-security identification and ID card" that "is the dream of the surveillance state."[39] China has used WeChat to crack down on anything which poses a threat to the harmony and stability of the state. For example, it has 75 behavioral indicators such as growing a beard or calling a relative overseas that allegedly indicate potential religious radicalization.[40] This is not merely a concern for China's citizens. Tencent, a China owned company that is one of the largest gaming companies in the world, owns major stakes in popular games like Fortnite (console-based), Riot

Games (pc games), and Supercell (mobile). Recently, the U.S. Congress has begun questioning what data is being gathered and collected by the company and sent back to China's servers.[41] Tiktok and Zoom have also come under scrutiny due to lack of clarity over what is gathered from individuals' devices and sent back to China. While Chinese data collection is perceived as a national security threat, domestic data collection is viewed as a digital privacy issue—these are not separate issues. Domestic digital privacy is fundamentally linked to national security.

MICROTARGETING AS INFORMATION WAR

The main difference between political microtargeting and military information operations is who is doing the targeting and who is the target. Information warfare is defined as "planned operations to 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 in a manner favorable to the originator's objectives."[42] There is very little difference between the methods of analysis, data collection, and actions used to influence behavior. Information warfare campaigns develop "insights on how best to persuade the target to change its behavior to one that is more favorable to US interests."[43] Consumer patterns used in advertising help reveal additional insights about a population such as life course events. One now notorious story about successful digital targeting of advertising is the story of a father who received advertising for babies only to discover that his daughter was pregnant. The algorithm knew before she had told him.[44]

The fact that one is used on perceived foreign adversaries, whereas one is used to sell the latest hot holiday toy or to influence elections, is a distinction without a difference. The objective of surveillance capitalism-enabled advertising and information warfare is the same: to influence an individual's behavior change in support of someone else's goals. In advertising, the goal is to motivate someone to make a purchase or sign up for a mailing list or otherwise take action related to the sale of a product. What happens when these tools are used for darker purposes?

Social media reveals what people attach themselves to and data-aggregated microtargeting has allowed it to be weaponized.[45] In the US, the digital advertising market is estimated to be worth over 32 billion as of 2017, and the vast majority of this spending is concentrated on Facebook and Google.[46] This is only the advertising spending—not the value of the data gathered and purchased. Recent independent investigations have raised questions about the accuracy of the ad campaigns on Facebook with Uber revealing they had cut their advertising budget by two thirds and saw no change in their engagement. The actual scope and value of this market are surprisingly difficult to measure, but using proxies, they can be estimated. For example, the smart home market, which includes things like Nest thermostat or Ring doorbell, is estimated to be worth "36 billion dollars in 2018 and expected to reach 151 billion by 2023."[47] The smart home market is an excellent example of the scale and scope of surveillance technologies.

Consider when Sarah Huckabee Sanders, the White House press secretary, tweeted about her 2-year-old being able to buy toys via Alexa.[48] Sanders informed the entire world that she—a person with direct daily access to the President of the United States—had what was functionally a listening device *in her home*. While there is no evidence her smart speaker was hacked, it remains a potent vulnerability for everyone.

The information extracted by the surveillance economy has granted anyone with the means to access these systems "direct access to the minds and lives of guards, clerks, girlfriends...a detailed trail of personal information that would previously have taken months of careful observation to gather."[49] Individual cell phone users can be tracked using location-based information updated in real time.[50] Recently, undergraduates at Harvard combined information available on the dark web with a purchased Experian database to identify nearly 1,000 high-net worth individuals in Washington, DC. "They were able to identify 1,000 people who have a high net worth, are married, have children, and also have a username or password on a cheating website. Another query pulled up a list of senior-level politicians, revealing the credit scores, phone numbers, and addresses of three U.S. Senators, three U.S. Representatives, the mayor of Washington, DC, and a Cabinet member."[51] The sheer magnitude of information commercially available on individuals at scale makes it critically important that researchers understand "which behaviors of large groups of people can be influenced by applying psychological mass persuasion—both in their interest and against their best interest."[52] This information is available legally from a wide variety of data brokers to anyone, including US adversaries.

ALGORITHMIC POLARIZATION

Fake news spreads faster than accurate news,[53] breaking down trust in institutions[54] that was already eroding over the last 40 years of growing economic inequality.[55] Following the Senate investigation into Russian election interference, the bipartisan, unclassified report detailed how Russian operatives targeted infrastructure during the 2016 US election using Facebook-targeted advertising.[56] Additionally, Russian active measures used social media to exacerbate existing cultural tensions within the US.[57] Not everyone was caught unaware: Black feminists online realized some accounts were masquerading as Black activists and quickly began working together to identify misinformation attempts with the hashtag #yourslipisshowing.[58] Social media content is optimized to produce polarizing content[59] and researchers have demonstrated the contagion effect of highly emotional content.[60] The social contagion effect of social media has been well documented. Facebook suffered an incredible backlash when it was revealed that it had manipulated people's emotions by choosing happy or sad post updates and then monitoring people's subsequent reactions.[61] Other research has demonstrated the contagion effect of domestic terror groups.[62] The US military is not immune to these polarization effects, creating a significant attack surface for adversaries to weaponize against DoD. And yet, the ability to understand the attack surface within DoD is limited by law, some of the only legal restrictions that exist restricting who can access these data.

OPERATIONAL VULNERABILITIES

DoD is legally restricted from "collecting intelligence against US persons" by Executive Order (E.O.) 12333.[63] This, along with service-specific regulations like Army Regulation 381-10, has been interpreted to restrict analysis of publicly available data such as the data gathered on social media platforms or other data brokers. While there are exceptions to these legislative restrictions, the Army has largely kept hands off of domestic social media or its understanding of the underlying data. The result of this is that there is no agency within the Army charged with understanding the ways in which US adversaries can manipulate the domestic information warfare space. Despite the fact that this data about US forces is readily available to our adversaries, the Army is unable to assess or respond to threats in the social media space. For example, when a recent case at Fort Hood involving missing soldier Vanessa Guillen went viral, Army leaders did not have the appropriate tools to understand the domestic social media situation, i.e., how the message was being amplified and spread.[64]

The restraint on the US government's ability to understand its own population's social media and digital footprint ignores the ability of other governments and other agencies to engage in this same behavior. *The New York Times* recently purchased cell phone data on over two million users and showed how it was able to individually track people to and from work at the Pentagon.[65] This regulatory gray zone also ignores how government agencies can contract around these restrictions. Recently, *The Wall Street Journal* reported that the Department of Homeland Security (DHS) had purchased commercially available cell phone location data to target undocumented immigrants.[66] The DoD is not completely unaware of these vulnerabilities and has purchased some of these databases in order to aid foreign operations.[67] After a Strava database leak revealed forward operating base perimeters due to personal GPS training devices, the military banned its use in deployed environments.[68] It has also banned the China-owned app TikTok from government cell phones but has not taken steps to prohibit soldiers from having it on their personal devices.[69] These are good first steps, but the implications are much bigger than specific apps or locations.

The misinformation environment is not only an overseas operational concern. The considerable misinformation surrounding masks during the COVID pandemic negatively impacted training and readiness for the military. Entire ships were docked as the crew became infected and the military infection rate in some cases exceeded the national level.[70] The military is made up of regular Americans and is not immune to the political debate about masks and freedom.[71] Algorithmic targeting of servicemembers with misinformation has a very different impact on national defense than on other communities, and these consequences do not disappear within the geographic boundaries of the US.

Military social media guidance offers limited utility in protecting users' data from data collection. Other than the U.S. Special Operations Command privacy quick reference guides sheets, there is no policy or directive outlining how soldiers can or should remove their information

from public databases such as Spokeo or others. Servicemembers are not advised to avoid popular but famously insecure email services like Gmail, Yahoo, or MSN. Soldiers receive no advanced warning about the risks of installing Facebook's Messenger on their phones, which gives the company access to their photos, contacts, location data, and messages.[72] Given the notorious difficulty of using DoD systems, forcing soldiers off free tools would likely backfire, but beyond that, any guidance targeted at the individual level is destined to fail. Collective efforts are necessary.

RECOMMENDATIONS

There is no way for any individual to tackle the surveillance economy.[73] Individual privacy is networked and connected.[74] Even if an individual does not have a Facebook account, Facebook has a shadow account for them,[75] collected from friends' phones, contact lists, and emails as well as data Facebook itself purchases. Privacy is not an individual effort; it is networked and requires networked solutions.[76] Location data cannot be turned off due to user requirements to ping the nearest cell phone tower and most apps fail to work if they don't have location data enabled. Additionally, the no/low cost of the current ad supported model enables public entities like schools to pivot online with little cost. Google Classroom, for example, offers cash-strapped school districts digital access but at the cost of children's privacy.[77] These tools are not inherently evil, but the lack of control and oversight over who can access their data, and with what data sets they can be combined, should be more highly scrutinized and regulated by governments. These tools are far beyond any individual's ability to manage.

The European Union's General Data Protection Regulation (GDPR) and the State of California have taken meaningful action to regulate the data privacy market, but these protections are only the beginning of what is required.[78] DoD should engage with the major social media companies to have them remove military servicemembers and their immediate family members from algorithmic targeting. DoD should also work with data brokers to prevent any servicemembers and their immediate families from having their data collected or sold. Companies that sell smart devices should be required to segregate data that comes from military households to prevent it from being converted into covert surveillance,[79] much as Furbies were once banned from secure facilities. The California Consumer Privacy Protection Act, which went into effect in 2020, allows individuals to request their information be deleted—DoD should preemptively do this for all servicemembers and families. Deleting this data would make it more difficult for individuals to be targeted for an online harassment campaign such as the sergeant accused by China of being COVID patient zero.[80] Preventing the data from being bought and sold would be another layer of protection for individuals.

Another recommendation is to limit the level of experimentation that social media companies conduct on the population. Social media companies should be subject to the same human experiment restrictions as academic institutions and medical companies. Facebook has

conducted psychological experiments on emotional contagion,[81] and the platforms are constantly being tested and revised to optimize for capturing attention. More insidiously, however, are reported Cambridge Analytica experiments that evaluated the relationships between personality and political outcomes[82] and also targeted "those who were more prone to impulsive anger or conspiratorial thinking"[83] with messages designed to inflame and provoke them, all without any meaningful informed consent. Medical companies and academic institutions are not allowed to conduct research on human subjects without informed consent and oversight to determine whether the value of the experiment is greater than the potential harm. Human subjects research was first limited after the horrors of the experimentation conducted under the Nuremberg Laws. Psychological manipulation research by the government, universities, and hospitals is dramatically limited due to concerns over individual autonomy, meaningful consent, and abusive practices.[84] Social media companies' experiments on populations should be held to the same oversight and regulation as hospitals and academic research in order to provide oversight and prevent harm.

Furthermore, the algorithms being used are opaque and not widely understood. Recent research has demonstrated how the Russians have weaponized fake military profiles against constitutional foundations such as the right to protest or certain political parties,[85] eroding US citizens trust in their military and their government. These social media companies have "allowed attack vectors on our societal cohesion...[given] direct access to the minds of US citizens."[86] Given that social media has been linked to genocide,[87] any future changes to the platforms should be halted until the algorithms' effects on individuals and society are better understood.[88] No military in its right mind would allow its servicemembers to be experimented on; yet, that is exactly what happens every day with misinformation on social media.

Part of this oversight should be to require researchers be given direct access to data and algorithms in order to understand the social and psychological aspects of social media microtargeting. There are very real questions about the validity of the claims made by these marketing companies.[89] If data is not the promised new oil but rather snake oil, governments have an obligation to reign in a potentially fraudulent market.[90] Currently, researchers are limited to what data is released by the platforms and are unable to meaningful replicate studies to test whether private companies like Cambridge Analytica actually manipulated election outcomes.[91]

Academic researchers are unable ethically to conduct the same experiments Facebook and other companies have performed and these companies should be required to grant access to universities and government agencies in order to determine what worked and how to defend against these tactics in the future. Access to this data should be highly restricted given national security concerns.

CONCLUSION

Information microtargeting, surveillance capitalism, modern advertising, and foreign influence operations are essentially synonymous and represent a national security concern that DoD and the rest of the federal government must address. In today's media environment, however, "if you make it trend, you make it true."[92] The ability to target the trending message toward people more likely to be receptive to it reduces national security and further erodes already weakened trust in institutions. Because nearly all of this data is available for purchase by anyone, surveillance capitalism has opened up an information warfare attack space on the American people, one the DoD is currently unprepared to defend. While there are limitations to what messages the US government can target at its citizens,[93] there are very few limitations on what foreign governments can target toward other populations. Current limitations are based on terms of service violations rather than national security concerns. This should stop. Facebook founder Mark Zuckerberg has stated that his company will not fact check political advertisements.[94] It has outsourced its content moderation to contractors, several of whom suffer from PTSD due to the horrors of the content to which they have been exposed.[95] Zuckerberg argues that Facebook's success is patriotic in order to stand as a bulwark against China's dominance[96]—this a deflection attempt disguising the fact that Facebook serves its own ends and not national interests.[97] There is bipartisan acknowledgment that Russia sponsored several disinformation campaigns within US geographic boundaries during the 2016 campaign.[98] Facebook initially dismissed these claims, but, as evidence mounted, it was forced to acknowledge abuse of its system.[99]

The microtargeting environment enabled by surveillance capitalism sacrifices collective security in the name of a free-market economy. Governments must wrestle with the implications of the surveillance economy sooner rather than later. This pits the interests of the companies—profit—against the Constitution and interests of national security. This is a false dichotomy. Profit tends to do better in a stable society—destabilized societies do not buy things on the Internet. There is nothing in the Constitution that prevents the government from regulating industries, especially dangerous industries and their products. For all the good these technologies have enabled, there is ample evidence that they are enabling the erosion of the foundations of freedom and democracy. Since most of these companies are based in the US, taking meaningful action to limit their reach and power over American citizens' digital lives would have meaningful global impact. It would also reestablish the US global commitment to values such as freedom and democracy by reigning in tools currently being used to undermine both. It would also offer an alternative to the global worldview of the People's Republic of China that prioritizes harmony aligned with China's interests over any conception of human rights and uses vast digital surveillance to accomplish this compliance.

NOTES

1. Bryan Sparling, "The Zhenhua Leak, IOS 14 and National Security.," LinkedIn, September 24, 2020, https://www.linkedin.com/pulse/zhenhua-leak-ios-14-national-security-bryan-sparling.
2. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power,* 1st edition (Location?PublicAffairs, 2019), 8.
3. Christopher Wylie, *Mindf*ck: Cambridge Analytica and the Plot to Break America* (New York: Random House, 2019); Brittany Kaiser, *Targeted: The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again* (Location?Harper, 2019); Sasha Issenberg, *The Victory Lab: The Secret Science of Winning Campaigns,* Reprint edition (New York: Broadway Books, 2013).
4. Zeynep Tufekci, *Twitter and Tear Gas: The Power and Fragility of Networked Protest*, Reprint edition (New Haven, CT: Yale University Press, 2018).
5. "Communications Decency Act," 47 U.S. Code § 230, accessed November 19, 2020, https://www.law.cornell.edu/uscode/text/47/230.
6. Facebook, "Case Study: Reaching Voters with Facebook Ads (Vote No on 8)" (Menlo Park, CA: Facebook for Government, Politics & Advocacy, July 2011), https://www.facebook.com/notes/us-politics-on-facebook/case-study-reaching-voters-with-facebook-ads-vote-no-on-8/10150257619200882.
7. Channel 4 News InvestigationsTeam, "Revealed: Trump Campaign Strategy to Deter Millions of Black Americans from Voting in 2016," Channel 4 News, September 28, 2020, https://www.channel4.com/news/revealed-trump-campaign-strategy-to-deter-millions-of-black-americans-from-voting-in-2016.
8. Dan Patterson, "Trolls Are Spreading Conspiracy Theories That a US Army Reservist Is 'COVID-19 Patient Zero,' China Is Amplifying That Disinformation," *CBS Evening News*, April 30, 2020, online edition, https://www.cbsnews.com/news/coronavirus-patient-zero-china-trolls/.
9. Brittany Kaiser, *Targeted: The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again*, Harper, 2019, 57.
10. Tim Hwang, *Subprime Attention Crisis: Advertising and the Time Bomb at the Heart of the Internet* (New York: FSG Originals, 2020); Zeynep Tufekci, "Opinion | The Looming Digital Meltdown," *The New York Times*, January 6, 2018, https://www.nytimes.com/2018/01/06/opinion/looming-digital-meltdown.html.
11. Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, 1st edition (New York: W.W. Norton & Company, 2016).
12. Michael Schudson, *Advertising, The Uneasy Persuasion: Its Dubious Impact On American Society*, Reprint edition (New York: Basic Books, 1986), xx.
13. Zuboff, T*he Age of Surveillance Capitalism*, 78.
14. Zuboff, 20.
15. Zuboff, 8.
16. Schudson, *Advertising, The Uneasy Persuasion,* xxi.
17. Hwang, *Subprime Attention Crisis*; Vincent F. Hendricks and Mads Vestergaard, "The Attention Economy," in Reality Lost: Markets of Attention, Misinformation and Manipulation, ed. Vincent F. Hendricks and Mads Vestergaard (Cham, Switzerland: Springer International Publishing, 2019), 1-17, https://doi.org/10.1007/978-3-030-00813-0_1.
18. Martin Gilens, "Gender and Support for Reagan: A Comprehensive Model of Presidential Approval," American Journal of Political Science 32, no. 1 (1988): 19-49, https://doi.org/10.2307/2111308.
19. Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Reprint edition (New York: Broadway Books, 2017).
20. Cambridge Analytica, "Key Case Studies" (Cambridge Analytica, 2015).
21. David Beer, "The Social Power of Algorithms," I*nformation, Communication & Society* 20, no. 1 (January 2, 2017): 4, https://doi.org/10.1080/1369118X.2016.1216147.
22. Kaiser, *Targeted,* 136.
23. Wylie, *Mindf*ck*.
24. Craig Silverman and Ryan Mac, "Facebook Gets Rich Off Of Ads That Rip Off Its Users," BuzzFeed News, December 10, 2020, https://www.buzzfeednews.com/article/craigsilverman/facebook-ad-scams-revenue-china-tiktok-vietnam.
25. Kaiser, *Targeted*, 398.
26. Robert L. Mitchell, "What Google Knows About You," Computerworld, May 11, 2009, https://www.computerworld.com/article/2551008/what-google-knows-about-you.html.

NOTES

27. Hendricks and Vestergaard, "The Attention Economy"; Zeynep Tufekci, "View of Engineering the Public: Big Data, Surveillance and Computational Politics | *First Monday*," First Monday 19, no. 7 (2014), https://firstmonday.org/ojs/index.php/fm/article/view/4901/4097.
28 DARPA, "Narrative Networks,". Defense Advanced Research Projects Agency, 2011, https://www.darpa.mil/program/narrative-networks.
29. Wylie, *Mindf*ck*; Kaiser, *Targeted*; Cambridge Analytica, "Key Case Studies."
30. Alan S. Gerber et al., "The Big Five Personality Traits in the Political Arena," *Annual Review of Political Science* 14, no. 1 (June 15, 2011): 265-87, https://doi.org/10.1146/annurev-polisci-051010-111659.
31. Wylie, Mindf*ck, 24.
32. Kaiser, *Targeted*; Wylie, *Mindf*ck*; Issenberg, *The Victory Lab.*
33. Kaiser, *Targeted*, 398.
34. Wylie, M*indf*ck*, 72.
35. Wylie, *Mindf*ck.*
36. S. C. Matz et al., "Psychological Targeting as an Effective Approach to Digital Mass Persuasion," Proceedings of the National Academy of Sciences 114, no. 48 (November 28, 2017): 12714, PAGE Number? https://doi.org/10.1073/pnas.1710966114.
37. Wylie, *Mindf*ck.*
38. Kai Strittmatter, *We Have Been Harmonized: Life in China's Surveillance State* (LOCATION?Custom House, 2020), 186.
39. Strittmatter, 187.
40. Strittmatter, *We Have Been Harmonized.*
41. Jenny Leonard, Saleha Mohsin, and David McLaughlin, "Tencent's Gaming Stakes Draw U.S. National Security Scrutiny," MSN, 2020, https://www.msn.com/en-us/money/other/tencents-gaming-stakes-draw-us-national-security-scrutiny/ar-BB199H8k.
42. "Joint Publication 3-13.2: Military Information Support Operations" (U.S. Department of Defense, December 20, 2011), https://www.bits.de/NRANEU/others/jp-doctrine/JP3-13.2C1(11).pdf.
43. "Joint Publication 3-13.2: Military Information Support Operations."
44. Schneier, *Data and Goliath.*
45. Wylie, *Mindf*ck*, 67.
46. Hwang, *Subprime Attention Crisis*, 13.
47. Zuboff, *The Age of Surveillance Capitalism*, 6.
48. Anna Giaritelli, "Sarah Sanders Warns Amazon about Its Echo Device: 'We Have a Problem,'" *Washington Examiner*, January 15, 2018, https://www.washingtonexaminer.com/sarah-sanders-warns-amazon-about-its-echo-device-we-have-a-problem.
49. Wylie, *Mindf*ck*, 49.
50. Stuart A Thompson and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy," *The New York Times,* December 19, 2019, Online Edition edition.
51. Adam Zewe, "Imperiled Information: Students Find Website Data Leaks Pose Greater Risk than Most People Realize," Harvard John A. Paulson School of Engineering and Applied Sciences, January 17, 2020, https://www.seas.harvard.edu/news/2020/01/imperiled-information.
52. Matz et al., "Psychological Targeting as an Effective Approach to Digital Mass Persuasion," 12714.
53. Sandeep Suntwal, Susan A. Brown, and Mark W. Patton, "How Does Information Spread? A Study of True and Fake News," n.d., 10.
54. Francesca Polletta and Jessica Callahan, "Deep Stories, Nostalgia Narratives, and Fake News: Storytelling in the Trump Era," *American Journal of Cultural Sociology* 5, no. 3 (October 2017): 392-408, https://doi.org/10.1057/s41290-017-0037-7.
55. Joseph E. Stiglitz, *The Price of Inequality: How Today's Divided Society Endangers Our Future,* 1 edition (New York: W. W. Norton & Company, 2012).do you have a page number?
56. 116th Congress, "REPORT OF THE SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE ON RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION," Senate Report (Washington, DC: United States Senate Intelligence Committee, 2017), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

NOTES

57. Claire Allbright, "A Russian Facebook Page Organized a Protest in Texas. A Different Russian Page Launched the Counterprotest," *The Texas Tribune*, November 1, 2017, https://www.texastribune.org/2017/11/01/russian-facebook-page-organized-protest-texas-different-russian-page-1/; Andrew Weisburd, Clint Watts, and JM Berger, "Trolling for Trump: How Russia Is Trying to Destroy Our Democracy," *War on the Rocks*, November 6, 2016; Ryan Browne, "Russian Trolls Tried to Convince African Americans Not to Vote in 2016, US Senate Says," CNBC, October 9, 2019, https://www.cnbc.com/2019/10/09/senate-intel-report-russian-trolls-targeted-african-americans-in-2016.html.
58. Rachelle Hampton, "Years Ago, Black Feminists Worked Together to Unmask Twitter Trolls Posing as Women of Color. If Only More People Paid Attention," *Slate Magazine*, April 23, 2019, https://slate.com/technology/2019/04/black-feminists-alt-right-twitter-gamergate.html.
59. Zeynep Tufekci, "Opinion | YouTube, the Great Radicalizer," *The New York Times*, March 10, 2018, https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html.
60. Amit Goldenberg and James Gross, "Digital Emotion Contagion," accessed October 8, 2019, https://doi.org/10.31219/osf.io/53bdu; A.D.I. Kramer, J.E. Guillory, and J.T. Hancock, "Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks," *Proceedings of the National Academy of Sciences* 111, no. 24 (June 17, 2014): 8788-90, https://doi.org/10.1073/pnas.1320040111.
61. Adam D.I. Kramer, "The Spread of Emotion via Facebook," in *Proceedings of the 2012 ACM Annual Conference on Human Factors in Computing Systems - CHI '12* (the 2012 ACM annual conference, Austin, TX: ACM Press, 2012), 767, https://doi.org/10.1145/2207676.2207787; Kramer, Guillory, and Hancock, "Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks."
62. Alex Goldenberg and Joel Finkelstein, "Cyber Swarming, Memetic Warfare and Viral Insurgency: How Domestic Militants Organize on Memes to Incite Violent Insurrection and Terror Against Government and Law Enforcement" (Princeton, NJ: Network Contagion Research Institute, 2020).
63. William Johnson, ed., *Operational Law Handbook* (Charlottesville, VA: Judge Advocate General's Legal Center and School, 2013), 105.
64. Heather Osborne and Jessica Priest, "Vanessa Guillen's Killing at Fort Hood Leaves Family Grieving, Grasping for Clues," MSN, July 18, 2020, Online edition, https://www.msn.com/en-us/news/us/vanessa-guillens-killing-at-fort-hood-leaves-family-grieving-grasping-for-clues/ar-BB16RNIl; Jim Hice, "New Leadership Named on Fort Hood in Response to Vanessa Guillen Case," MSN, September 1, 2020, https://www.msn.com/en-us/news/us/new-leadership-named-on-fort-hood-in-response-to-vanessa-guillen-case/ar-BB18ByD7.
65. Thompson and Warzel, "Twelve Million Phones, One Dataset, Zero Privacy."
66. Byron Tau and Michelle Hackman, "WSJ News Exclusive | Federal Agencies Use Cellphone Location Data for Immigration Enforcement," *The Wall Street Journal*, February 7, 2020, sec. Politics, https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600.
67. Joseph Cox, "How the U.S. Military Buys Location Data from Ordinary Apps," Vice.com, November 16, 2020, https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x.
68. Matt Burgess, "Strava's Data Lets Anyone See the Names (and Heart Rates) of People Exercising on Military Bases," *Wired UK*, January 30, 2018, https://www.wired.co.uk/article/strava-military-bases-area-51-map-afghanistan-gchq-military.
69. Josephine Wolff, "The Military's Ban of TikTok Is Just the Beginning," *Slate Magazine*, January 6, 2020, https://slate.com/technology/2020/01/military-tiktok-ban-strava-genetic-testing.html.
70. Gina Harkins, "6 Big Takeaways from the Full Navy Investigation into a Carrier's COVID Outbreak," Military.com, September 19, 2020, https://www.military.com/daily-news/2020/09/19/6-big-takeaways-full-navy-investigation-carriers-covid-outbreak.html; Meghann Myers, "Military's COVID-19 Cases Growing at Twice the Nationwide Rate," *Military Times*, July 13, 2020, https://www.militarytimes.com/news/your-military/2020/07/10/militarys-covid-19-cases-growing-at-twice-the-nationwide-rate/.
71. Eric Taylor Woods et al., "COVID-19, Nationalism, and the Politics of Crisis: A Scholarly Exchange," *Nations and Nationalism*, July 19, 2020, https://doi.org/10.1111/nana.12644.
72. Zak Doffman, "Why You Should Stop Using Facebook Messenger," *Forbes*, July 25, 2020, https://www.forbes.com/sites/zakdoffman/2020/07/25/why-you-should-stop-using-facebook-messenger-encryption-whatsapp-update-twitter-hack/.
73. Zeynep Tufekci, "Opinion | Think You're Discreet Online? Think Again," *The New York Times*, April 21, 2019, https://www.nytimes.com/2019/04/21/opinion/computational-inference.html.

NOTES

74. Sara Bannerman, "Relational Privacy and the Networked Governance of the Self," *Information, Communication & Society* 22, no. 14 (December 6, 2019): 2187-2202, https://doi.org/10.1080/1369118X.2018.1478982; Juniper Lovato et al., "Distributed Consent and Its Impact on Privacy and Observability in Social Networks," *ArXiv:2006.16140 [Physics]*, June 29, 2020, http://arxiv.org/abs/2006.16140; Tufekci, *Twitter and Tear Gas.*
75. Kate Knibbs, "What Is a Facebook Shadow Profile," Digital Trends, July 5, 2013, https://www.digitaltrends.com/social-media/what-exactly-is-a-facebook-shadow-profile/.
76. Tufekci, "Opinion | Think You're Discreet Online?"
77. Sara Morrison, "Google's Education Tech Has a Privacy Problem," Vox, February 21, 2020, https://www.vox.com/recode/2020/2/21/21146998/google-new-mexico-children-privacy-school-chromebook-lawsuit.
78. Xavier Becerra, "California Consumer Privacy Act (CCPA)" (State of California, 2020), https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-third-set-mod-101220.pdf?
79. Kimiko de Freytas-Tamura, "The Bright-Eyed Talking Doll That Just Might Be a Spy (Published 2017)," T*he New York Times*, February 17, 2017, https://www.nytimes.com/2017/02/17/technology/cayla-talking-doll-hackers.html; Lauren Davis, "The NSA Once Banned Furbies as a Threat to National Security," io9, February 20, 2014, https://io9.gizmodo.com/the-nsa-once-banned-furbies-as-a-threat-to-national-sec-1526908210.
80. Dan Patterson, "Trolls Are Spreading Conspiracy Theories That a U.S. Army Reservist Is 'COVID-19 Patient Zero' China Is Amplifying That Disinformation.," CBS News, April 30, 2020, https://www.cbsnews.com/news/coronavirus-patient-zero-china-trolls/.
81. Kramer, "The Spread of Emotion via Facebook."
82. Wylie, *Mindf*ck.*
83. Wylie, 120.
84. "45 CFR 46 (Protection of Human Subjects)" (United States Government, 1991).
85. Dana Weinberg and Jessica Dawson, Ph.D., "From Anti-Vaxxer Moms to Militia Men: Influence Operations, Narrative Weaponization, and the Fracturing of American Identity" (SocArXiv, October 30, 2020), https://doi.org/10.31235/osf.io/87zmk.
86. Renny Gleeson, "Truth Dies First: Storyweapons on the InfoOps Battlefield," *The Cyber Defense Review* (Summer 2020): 71.
87. Marzuki Darusman, "OHCHR | Statement by Mr. Marzuki DARUSMAN, Chairperson of the Independent International Fact-Finding Mission on Myanmar, at the 37th Session of the Human Rights Council" (2018), https://www.ohchr.org/EN/HRBodies/HRC/Pages/NewsDetail.aspx?NewsID=22798&LangID=E.
88. Marietje Schaake, "Trade Secrets Shouldn't Shield Tech Companies' Algorithms from Oversight," Brookings (blog), May 4, 2020, https://www.brookings.edu/techstream/trade-secrets-shouldnt-shield-tech-companies-algorithms-from-oversight/.
89. Hwang, *Subprime Attention Crisis.*
90. Hwang; Jeroen van Zeeland, "Data Is Not the New Oil," *Medium*, December 7, 2019, https://towardsdatascience.com/data-is-not-the-new-oil-721f5109851b; Cory Doctorow, "How to Destroy 'Surveillance Capitalism,'" *Medium*, August 30, 2020, https://onezero.medium.com/how-to-destroy-surveillance-capitalism-8135e6744d59.
91. Vian Bakir, "Psychological Operations in Digital Political Campaigns: Assessing Cambridge Analytica's Psychographic Profiling and Targeting," F*rontiers in Communication* 5 (September 3, 2020): 67, https://doi.org/10.3389/fcomm.2020.00067; Cambridge Analytica, "Key Case Studies"; Doctorow, "How to Destroy 'Surveillance Capitalism.'"
92. Renee DiResta, "Computational Propaganda: If You Make It Trend, You Make It True," *The Yale Review*, October 9, 2018, https://yalereview.yale.edu/computational-propaganda.
93. Mac Thornberry, "H.R.5736 - 112th Congress (2011-2012): Smith-Mundt Modernization Act of 2012," webpage, May 10, 2012, https://www.congress.gov/bill/112th-congress/house-bill/5736.
94. David Klepper, "Facebook Clarifies Zuckerberg Remarks on False Political Ads," AP News, October 25, 2019, https://apnews.com/64fe06acd28145f5913d6f815bec36a2.
95. Casey Newton, "Three Facebook Moderators Break Their NDAs to Expose a Company in Crisis," The Verge, June 19, 2019, https://www.theverge.com/2019/6/19/18681845/facebook-moderator-interviews-video-trauma-ptsd-cognizant-tampa.

NOTES

96. Sarah Frier, "Zuckerberg to Tell Congress Facebook's Success Is Patriotic," Bloomberg, July 27, 2020, https://www.bloomberg.com/news/articles/2020-07-27/zuckerberg-to-tell-congress-facebook-s-success-is-patriotic.
97. Zeynep Tufekci, "Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency," *Colorado Technical Law Journal 13 (2015): 17; Zeynep Tufekci, "Opinion | Facebook's Surveillance Machine," The New York Times, March 19, 2018, sec. Opinion*, https://www.nytimes.com/2018/03/19/opinion/facebook-cambridge-analytica.html.
98. Allbright, "A Russian Facebook Page Organized a Protest in Texas. A Different Russian Page Launched the Counterprotest"; Browne, "Russian Trolls Tried to Convince African Americans Not to Vote in 2016, US Senate Says"; Weisburd, Watts, and Berger, "Trolling for Trump: How Russia Is Trying to Destroy Our Democracy."
99. Tufekci, "Opinion | Facebook's Surveillance Machine"; Carole Cadwalladr and Emma Graham-Harrison, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach," *The Guardian,* March 17, 2018, sec. News, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

The Promise of Strategic Gain in the Digital Information Age: What Happened?

Dr. Zac Rogers

ABSTRACT

For approximately thirty years an unanswered question has hung over the military enterprise of nation-states: As the digital information age progresses, should we construct a military for the information age, or should we construct an information age military? The former would be an old enterprise applying new tools to its roles and missions. The latter would be a *new enterprise*. The new tools would not only alter the roles and missions the military prosecutes; they would alter the primary purposeful activity of the modern military. The short answer is that militaries and the national security communities that support them have hedged, wary of the uncertainty which comes with complex change. Into this gap has grown a new type of insecurity – a type not confined to military affairs and national security but society-wide – which open societies in particular are yet to fully understand and, thus to develop an appropriate response. The formulation of an appropriate response ties directly back to the thirty-year question. The response, where it exists, is decidedly fragmented. A new addition to the associated lexicon—"cognitive warfare"—has made its way into the discussion and makes no pretense of being confined strictly to military affairs. While a topic of increasing interest, anything resembling a bounded and discrete set of meanings to be associated with cognitive warfare has yet to emerge and seems a way off. This article aims to address this omission and to take stock of how the national security, intelligence, and defense (NSID) communities might begin to approach a coherent understanding of cognitive security. It argues the conflation of operational information warfare with cognitive warfare is a category error that must be addressed first. The hubris of the early digital age provides a lesson to be avoided.

© 2021 Dr. Zac Rogers

Dr. Zac Rogers, PhD, is Research Lead at the Jeff Bleich Centre for the US Alliance in Digital Technology, Security, and Governance at Flinders University of South Australia. His research combines a traditional grounding in national security, intelligence, and defence with emerging fields of social cybersecurity, digital anthropology, and democratic resilience.

INTRODUCTION

For approximately thirty years an unanswered question has hung over the military enterprise of nation-states: As the digital information age progresses, should we construct a military for the information age, or should we construct an information age military? The former would be an old enterprise applying new tools to its roles and missions. The latter would be a *new enterprise*. The new tools would not only alter the roles and missions the military prosecutes; they would alter the primary purposeful activity of the modern military. The short answer is that militaries and the national security communities that support them have hedged, wary of the uncertainty which comes with complex change. Scholars of war will note that, at least since the Treaty of Westphalia, warfare ultimately has reflected the types of societies which mandate its conduct. However, as John Keegan notes, warrior culture follows society at a distance. In fact, "The distance can never be closed, for the culture of the warrior can never be that of civilisation itself."[1] Into this gap has grown a new type of insecurity, which society at large is yet to fully understand and for which it is yet to mandate an appropriate response. The formulation of an appropriate response ties directly back to the thirty-year question but contains a twist. As the military enterprise has interacted with, incorporated, and in some cases, offloaded capability and responsibility for military-technical innovation to private enterprise, society too is reorienting around those shifts. The roles and statuses of information technologies of control and violence, as a result, are no longer chiefly military business. Yet whose business are they? And how is this changing what we mean by security?

Three overlapping themes, Information Warfare (IW), Dominant Battlespace Knowledge (DBK), and Network-Centric Warfare (NCW), dominated discussion and debate about military-strategic affairs within the

national security, intelligence, and defense (NSID) communities of the United States, its allies, competitors, and adversaries throughout the 1990s. The associated discursive and extra-discursive practices were situated under the rubric of a "Revolution in Military Affairs" and were primarily driven by developments in the application of digital information and communication technologies (ICT) to NSID affairs.[12] Digital ICTs were of course entering every aspect of the civilian domain at the same time, leading to an abundance of scholarship and commentary on the dawning of a networked digital information age or various aspects and iterations of it.[3]

Well into its third decade, the digital age has brought about several variations on these early discussions and the expectations contained therein. In particular, the evolution of IW has, in recent publicly observable episodes, undergone a transformation. Associated in the past primarily with the military battlefield, IW leached into the civilian domain as strategic contests between nation-states in the digital information age became more comprehensive. Today IW is widely understood as endangering the functional viability of entire societies.[4] An explanation as to how this came about has not been forthcoming. The widespread public expectation remains that the NSID community is still in charge and is busy formulating the appropriate and proportionate response to a host of intrusions, influence operations, and outright attacks.

The response, where it exists, is decidedly fragmented, however. A new addition to the associated lexicon—"cognitive warfare"—has made its way into the discussion and makes no pretense of being confined strictly to military affairs. An early criticism of IW was that it seemed to incorporate an indistinct set of themes and boundaries. While a topic of increasing interest, anything resembling a bounded and discrete set of meanings to be associated with cognitive warfare has yet to emerge and seems a way off. This article addresses this omission and then proceeds to take stock of how NSID communities might approach a coherent understanding of cognitive security. It argues the conflation of operational information warfare with cognitive warfare is a category error which must be addressed first. The hubris of the early digital age provides a lesson to be avoided.

From the Information Edge to Cognitive Insecurity

A series of assertions published in *Foreign Affairs* in 1996 by renowned International Relations (IR) scholar Joseph Nye and then U.S. Navy Admiral William Owens captures the prevailing attitude among a good portion of the US NSID community regarding the strategic advantage expected to accrue to the US as the digital information age unfolded:

- Knowledge, more than ever before, is power. The one country that can best lead the information revolution will be more powerful than any other. For the foreseeable future, that country is the United States.
- (America's) subtle comparative advantage is its ability to collect, process, act upon, and disseminate information, an edge that will almost certainly grow over the next decade.

- This information advantage can help deter or defeat traditional military threats at relatively low cost.
- The information advantage can strengthen the intellectual link between U.S. foreign policy and military power and offer new ways of maintaining leadership in alliances and ad hoc coalitions.
- The United States can use its information resources to engage China, Russia, and other powerful states in security dialogues to prevent them from becoming hostile.[15]

Nye and Owens were expressing what much of the discourse on the digital age of the 1990s had, by the turn of the century, taken as a near-certainty.[6] This cannot be passed off as mere media or academic hype. As Carl Builder noted, it was primarily factions within the US military determined to convince those in and out of uniform who held the purse strings that this was real.[7] Summarily, the prevailing view was that as humanity collectively moved from the industrial age to the information age, from industrial societies to information societies, from industrial warfare to information warfare, and from industrial economies to "knowledge" economies, the investments the US had made in a regime of digital ICTs during the Cold War were set to pay off in spades. The ICT edge was not only militarily relevant—its reach was far broader, and is now even more so.

Like much of post-war defense-led development, digital technology was naively dual-use and would likely magnify advantages as it was incorporated across each sector of society. The profound challenge to organizational structures presented by the digital age would likely also accrue to America's advantage–its open culture and rule of law, entrepreneurial spirit, commitment to market mechanisms, and reification of innovation was not a set of conditions enjoyed by any of its competitors.[8] The digital age would likely multiply US advantage in all these areas, leading to a cascade of advantages shared with allies, with which no rival to US dominance could hope to compete.[9]

If used wisely, the US could leverage its dominance not only to deter open military aggression but to dissuade competitors from even embarking down a path toward direct rivalry.[10] In this way, the US could perhaps become an efficient manager, rather than a costly enforcer, of an increasingly benign post-Cold War international order.[11] While a contentious assertion, the way seemed open, perhaps like never before, for commerce to shade geopolitics as the central theme of strategy and for American society to reap the rewards.[12] If any of this were so, not only the military's roles and missions but its purpose as an enterprise would be under serious review.[13]

The majority of the discourse from this time is rightly careful to point out the possible caveats and potential pitfalls of rushing to a digital future. The wave of enthusiasm, however, was difficult to deny. Barely twenty years on, and in the thick of a now ubiquitously insecure digital age, to reflect on these expectations is to experience a sense of vertigo. Expressing starkly contrasting sentiments, the 2018 US National Defense Strategy states:

> Today, we are emerging from a period of strategic atrophy, aware that our competitive military advantage has been eroding. We are facing increased global disorder, characterized by decline in the long-standing rules-based international order—creating a security environment more complex and volatile than any we have experienced in recent memory. Inter-state strategic competition, not terrorism, is now the primary concern in U.S. national security.

Of the challenge to American society in the aftermath of Russian interference in the 2016 Presidential election,[14] former U.S. Director of National Intelligence James Clapper writes, "I believe the destiny of the American ideal is at stake."[15] Former NSA and CIA Director General Michael Hayden has described the processes which protect American society from the risk of Hobbesian chaos as being "under stress, and that many of the premises on which we have based our governance, policy, and security are now challenged, eroded, or simply gone."[16]

Scattered throughout the earlier discourse were several salient warnings for digital age enthusiasts. By the late 1990s these warnings increased. Among them, Martin Libicki noted that the quest to "illuminate the battlefield"[17] with a globally situated and connected grid augmented by digital ICTs, which would expedite US and allied networked operations and could make military aggression harder for adversaries to prosecute. This could also be undermined and repurposed as a medium for the propagation of information warfare that leads to a *greater* likelihood of violent confrontation.[18] A monograph produced by RAND Corporation in 1999, while claiming "these changes have affected the global balance of power in favor of the United States," also warned:

> Information that is readily available is available to friend and foe alike; a system that relies on communication can become useless if its ability to communicate is interfered with or destroyed. Because this reliance is so general, attacks on the information infrastructure can have widespread effects, both for the military and for society. And such attacks can come from a variety of sources, some difficult or impossible to identify.[19]

Either an illuminated and therefore less violent battlefield, or an insecure substrate of complex and interconnected vulnerabilities, could be the prevailing outcome of a digital age that cannot be quarantined from the civilian domain. Libicki wrote of the dilemma, "Some systems make it easier for nations to resolve their differences and trust one another; others, by their nature, exacerbate suspicion."[20] Twenty years ago Libicki wrote that the United States had a fundamental choice between these two national defense paths.[21] Builder wrote that the US military found itself torn between a conservative path, of executing existing roles and missions more effectively with the addition of digital ICTs, and a more radical path in which a new type of war and warrior would emerge.[22] Andrew Marshall warned at the same time of the deep uncertainty brought about by the complexity of the coming era.[23] The events of 2016 offer an opportunity to pause and evaluate which path has been taken and its implications.

Information warfare in the national security, intelligence, and defense space is incorporated by a large and multi-disciplinary discourse. Subject areas as diverse as international security and strategic studies, cyber studies, the fourth industrial revolution, and future warfare have all engaged with aspects of IW in often indistinct and overlapping ways.[24] Often the problem with IW is knowing what it is not. Recent events, for example 2016's election interference and 2020's Solarwinds exposure to name just two, have brought renewed attention to the subject, and naturally its concepts and assumptions are evolving as discursive and extra-discursive practices challenge the veracity of existing assumptions about the subject.[25]

Prior to this increased in attention, IW attracted a prolonged wave of consideration from the NSID communities in the United States and those of a host of US partners, competitors, and adversaries in the early 1990s.[26] The focus was concurrent with the increasing application of digital information and communication technologies to NSID affairs and the contemplation of the implications in both IR and Strategic Studies.[27] For militaries, the deluge of data brought on by these new technological inputs engendered a major rethinking about ways, means, and ends with regard to contemporary warfighting, captured by the shift from attrition-based to effects-based operations. Of the thinking behind the shift, Edward Smith, Jr., wrote the following:

> The world in which we live is and always has been complex and filled with ambiguities and uncertainties, and the most complex part of this world has always been man himself – a point that operations in Iraq and Afghanistan underscore every day. Yet, in spite of this pervasive non-linearity, military efforts have tended to focus on linear, attrition-based solutions to linear warfare problems that often have little to do with our messy reality. Effects-Based Operations (EBO) focus on the single most complex aspect of this world: human beings and human organizations.[28]

This shift engendered a mismatch with existing levels of analysis in which tactical, operational, and strategic ends, ways, and means could be usefully demarcated across physical domains for clarity, coordination, and efficiency of effort.[29] The shift from attrition to effects in an unprecedented information-rich environment was to make strategic competition a society-wide, information-centric totality.[30] The traditional strategic art, contending with others for survival on contested terms amid scarcity, would take place in this new materiality. Of EBO, Smith continues:

> They treat national power as a whole and consider its application not just to military operations but across the entire spectrum of competition and conflict from peacetime deterrence, to crisis response, to hostilities in all their varied forms, to the restoration of peace.[31]

Previously well-defined lines of demarcation between military and civilian domains and peace and war were being quietly demolished by forces driven and enabled by the digital age. Publicly available discourse stating this reality among US allies was scarce, perhaps for obvious

reasons, while competitors and adversaries seemed more comfortable making it clear.[32] The digital information age would bring many aspects of strategic competition among nation-states away from the battlefield and more into the civilian domain,[33] and its center of gravity would home in on the mind of the individual–the cognitive agent. As cognitive neuroscientists Moreno and Giordano have noted, the human brain has become the locus of contending in the 21st century.[34] A new term in line with this evolution—"cognitive warfare" (CW)—has recently been used by high-ranking military officials, discussed and debated by military practitioners in formal and informal settings, and is being grappled with by the NSID and academic communities at large.[35] In September 2017, Air Force Chief of Staff, General David L. Goldfein, remarked at the Air, Space, and Cyber Symposium, "We're transitioning from wars of attrition to wars of cognition."[36] At the 2016 DODIIS Worldwide conference, Director of the Defense Intelligence Agency, Lieutenant General Vincent R. Stewart remarked, "How do we win warfare in the information age when the emphasis is as much on the cognitive as much as it is on the kinetic?"[37] The ways in which CW is distinct from IW, if it is distinct, have not been clarified.

Defining the Difference

IW is a battle *for* information where CW is a battle *of* information. Unpacking this simple definition will reveal why this is so, and why CW is a so far under-acknowledged divergence from IW with significant ramifications for the NSID community. Conflating the two is a category error, which stifles understanding, and thus development of the appropriate response. All aspects of operational IW involve actors contending over information within specified and assigned contexts in which the orientation of the context to the contending is settled. CW, conversely, involves actors contending within unspecified and unassigned contexts, in which the orientation of the context literally is the contest. The specification and assignment of context to information is what first gives it meaning, into which a contest can be entered by human actors—it is information which has been de-alienated by a cognitive process. Unspecified and unassigned information exists alienated from context—the contest shifts to the very process of de-alienation in which the information acquires its meaning. It is a cognitive contest and highly asymmetric in favor of the spoiler.

CW is really nothing like "warfare" at all, if we allow for the general heuristic that warfare normally involves contending parties knowingly engaged in the act of contending. Each party understands the context in its own way, but the context represents a minimal shared understanding that a contest has been entered into by the parties concerned. CW to date has been something more akin to terrorism or insurgency, whereby parties are engaged in continuous political opposition punctuated by infrequent acts of public violence against others to cause some often unspecified or frequently amended change in the behavior of the opposing polity. Though these are imperfect analogies. We will need to develop an understanding of a heterogenous type of cognitive violence which can be at once public and deeply private, non-lethal and highly destructive to human intellectual, emotional, and psychological states, blunt and undi-

rected as well as precise and tailored, and most times non-kinetic in the traditional military sense. The type of cognitive violence in mind can easily cause major disruption in the normal functioning of societies as well as significant changes in behavior without being assigned a specified meaning.[38] As Rand Waltzman urged, the time to specify and assign a new cognitive security paradigm is now.[39]

In 1995, Libicki wrote of information warfare, "All forms of struggle over control and dominance of information are considered essentially one struggle, and the techniques of information warfare are seen as aspects of a single discipline."[40] It is difficult to imagine a more all-encompassing description. The official DoD definition did not fare much better on detail. IW was described as:

> Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks.[41]

These actions were distinguished in practice by NSID communities into overlapping sub-categories, all involving the protection, manipulation, degradation, and denial of information, and could range from the analog to the digital, be transmitted via anything from carbon to silicon, and could manifest in the oldest forms of conflict to the newest technologies.[42] This taxonomy reflected a unique puzzle regarding information warfare that persists to the present day: if it can be everything at once, what is it not? In what sense and under what terms does it have a beginning and an end? Would battle be joined deliberately or by accident? This enduring puzzle produces another unhelpful problem: if information warfare is essentially indefinable, any definition that does tend to stick will be one imposed on it, often by a single constituency or the most motivated actor. In many ways, this has been the case with IW since the mid-1990s. Alvin Toffler and Heidi Toffler foresaw this predicament in *War and Anti-War* in 1993.[43] Viewing the history of warfare as essentially reflecting the incumbent society's mode of production, the emerging information age would inevitably be the age of an unrestricted and ill-defined new paradigm of information war.

Military organizations most often speak of the struggle for information in the context of the quest for operational situational awareness and in aid of weapon performance. Not particularly advantageous on its own, situational awareness is the foundation of the pursuit of "dominant battlespace knowledge" (DBK).[44] DBK connotes the cognitive capacity required to make effective use of superior situational awareness—to enable and augment the delivery of lethal effects on the battlefield while defending friendly forces from attack. The struggle for information has been understood as involving both offensive and defensive measures, including lines of effort in ISR (Intelligence, surveillance and reconnaissance), EW (electronic warfare), IO (information operations), CyberOps (cyber operations), and PsyOps (psychological operations), conducted to enable the lethal activities common to military organizations.[45] IW in the military domain has

been conducted under the rubric of both conventional and unconventional war involving both regular and irregular forces.[46] These represent specified and assigned modalities of contestation because they are conducted at the operational level.

As Libicki explains, however, while the imperative to conduct lines of IW effort under a unified construct has been acknowledged by US and allied forces since the 1990s, no such unity of effort has emerged despite significant effort, and each line of effort continues to be conducted by separate services in contingent and episodic fashion.[47] Significant advances in each line of effort have been achieved over that time, particularly in the years since 9/11,[48] without the emergence of a coherent and viable framework whereby network effects can leverage the much-desired dominant battle space knowledge. IW efforts have not been unified into a strategic main effort. This is not a failing: it should be understood as a category error that reflects the inherent tension between the two paths noted earlier.

Cognition is at the center of all modes of contending, a foundational assertion in the work of renowned military thinker John Boyd.[49] Boyd's OODA (observe–orient–decide–act) loop is a well known concept within military organizations and beyond, yet arguably its most pivotal element is often overlooked.[50] The core of the OODA loop is the second "O"—orientation. The capacity to observe, decide, and act is meaningless in any form of contending between humans if orientation is left unaddressed. Herein lie the consequences of category error. Orientation is central because any form of contending for information which occurs under conditions of complexity cannot assume the stability of those conditions and therefore the context in which the contending is occurring.

The most fundamental strategic assumption one can make concerns the cognitive conditions in which the contest is occurring—the orientation of the contenders with regard to reality. Arguably Boyd's most fundamental insight, drawing upon and synthesizing a multidisciplinary scientific and philosophical discourse,[51] was that the assumptions of scientific realism, the orientation under which reality is considered a discrete system of objects to which transient human subjects attempt to gain veridical access, is a cognitive weakness and a potentially exploitable vulnerability. Robert Coram summarized the centrality of orientation as follows: "Any inward-oriented and continued effort to improve the match-up of a concept with observed reality will only increase the degree of mismatch."[52] The assumptions of scientific realism applied to complex strategic contending between humans increase the risk of mismatch.[53]

IW, in the way it is conceived and fielded by military organizations, is categorically operational IW. It is in essence a set of inward-oriented and continuous efforts. These efforts have pre-specified and pre-assigned utility and function associated directly or indirectly with supporting the delivery of lethal effects on the battlefield. It is a category error to associate operational IW with the challenge of cognitive security, which has been brought on by the demolishing of boundaries in the digital age. Boyd and others knew that, as information flooded the modern warfighter in the digital age, it would quickly become an impediment if the cognitive

element was not prioritized. DBK is aimed at this goal. However, when strategic contending occurs via unspecified and unassigned modalities which treat the spatial-temporal locus of the contest as everywhere and all the time, as Smith conjectured, DBK does not exhaust the boundaries of the contest. The orientation is the contest. It determines the context and therefore the boundaries of the contest. Operational IW is Popperian science.[54] Cognitive security needs to be Polanyian-Kuhnian science.[55]

The potential of network effects, emerging in parallel with IW and part of the discourse on the digital age (also known as the network age), was also a hugely popular concept from the late 1990s.[56] Proponents of network-centric warfare envisioned an information-rich infrastructure delivering DBK not only to a network of US forces but potentially across allied coalition networks, vastly expanding the capacity to meet future threats to security with a more evenly shared burden of costs and risks.[57] Like IW, NCW struggled to transform from theory to practice. The US has repackaged NCW into its Multi-Domain Operations concept, which is highly derivative of the former.[58] Most contemporary militaries today remain committed to a version of networked warfare, while the scope and scale of early hopes have been dimmed by hard limits on its realization—constraints often more political in nature than technical.[59] Despite some extraordinarily lofty expectations, for the US and allied NSID communities, IW in the digital age is an operational contest for electrons stored in and transiting the electromagnetic spectrum (EMS) via silicon-based infrastructures as adjunct to achieving lethal battlefield effects, the object of the main military effort.

US and allied battlefield experiences in South and Central Asia and the Middle East since 2001 have honed and refined aspects of IW lines of effort, while much of the anticipated strategic level from the domination of digital age warfare is difficult to ascertain. Many would contend it does not exist and has become, in fact, a strategic liability as cognitive insecurity has gripped many of the polities for which the strategic gain was primarily intended.[60] Further iterations of NCW in aid of situational awareness, DBK, and IW, will continue to meet specified and assigned military utility.[61] They will not address the needs of cognitive security. Cognitive security must be assigned a separate category.

Option Dominance?

A review of the discourse on the early military-strategic expectations associated with IW, DBK, and NCW reveals a tale of missed opportunities, if not outright concept failure. That expectations were high is an understatement. According to then Admiral William Owens, writing in 1995, the US could expect to be:

> On the other side of this new revolution in military affairs years, perhaps decades, before any other nation. This is important for many reasons; one of the most significant is that completing the revolution offers us the opportunity to shape the international environment, rather than simply react to it.[62]

All authors writing on these concepts were careful to acknowledge the risks, potential vulnerabilities, and obstacles regarding the pursuit of rapid and highly innovative military transformation. Long lists of technical, political, and organizational challenges were readily admitted. The fundamental view, however, was not readily questioned: the quest to leverage the already extensive US advantage in digital age warfare would lead to outsized strategic gain. The most compelling of these arguments was centered on the concept described by David Alberts as "option dominance".[63] To summarize, option dominance referred to the expectation that, even allowing for the maximum level of push-back across each of the technical, political, and organizational challenge areas, strategic gain would accrue to the US and perhaps a select group of allies and partners.

The source of this relative gain was in the tendency for actors, who might be able to compete and even gain asymmetric advantages in narrow channels of digital age warfare, to be maneuvered nonetheless into a military-technical strategic cul-de-sac by US and allied dominance. Thus, any asymmetric gain would accrue an opportunity cost, which is why Libicki described such methods as second-best.[64] Each opportunity an adversary is forced to forfeit accrues a strategic gain to the dominant actor. The next asymmetric gain forfeits another opportunity cost and so on until the weaker adversary is forced to come to strategic terms in which the dominant military-technical actor holds all the cards. Option dominance was at the heart of NSID community expectations about the military/strategic-level contest likely to play out as the digital age swept through military organizations.[65]

In comments at the beginning of the 1999 RAND monograph, Andrew Marshall delivers what might be the discourse's most overlooked statement: "Information advances will affect more than just how we fight wars. *The nature and purpose of war itself may change.*"[66] The most obvious flaw in the option dominance thesis is that it assumes stability in the context under which the strategic competition is being conducted. An example of inward orientation, it assumes a finite set of options. The assumption of finitude is essential in narrow and discrete contests. It is a liability in open and complex contests. The literature on digital age warfare from the 1990s is more or less unanimous in the implied expectation that its fundamental purpose will be to facilitate application of lethal military force on the physical battlefield. Some allowance for unexpected developments is conveyed, but even the potential for a "black swan" event is understood within the context of the primacy of the lethal contest from which all other political and strategic ends are enabled.

This orientation toward the nature of war has been among the least challenged items in the canon of western military and strategic thought. It atrophies beneath the deep institutional faith in technological supremacy,[67] a well-documented feature of the US orientation toward strategic power (despite Boyd's influence). The costly assumption remains that the most consequential black swan event will be one that emerges in the realm of technology.[68] Unfortunately, the uncertainty about the nature and purpose of strategy to which Marshall was referring

entangles humans with shifting technologies in a complex matrix. A technology-driven black swan has emerged, but under a different orientation. The hyper-connectivity which has accompanied the digital age has exacerbated this condition markedly. As observed by Jeff Reilly, "Advances in technology have subtly nudged the entire globe into a realm where all previous notions of the battle space have been radically altered by domain interdependence."[69]

Cognitive Insecurity is the Hyper-War Offset

The cultivation of "optionality," as expounded by Nassim Nicholas Taleb, is a fundamental strategic necessity in any complex contest.[70] In short, optionality is the ability to discard failure without catastrophic cost while retaining the upside of what is learned. The concept of option dominance has failed because the US and allied NSID communities became unwittingly *obliged to keep* the diminishing strategic returns of the information age. The concept lost its optionality, the ability to *discard* adverse outcomes before they accumulate. The vulnerabilities inherent in the digital substrate highlighted by many early observers have outweighed the benefits, however one might conceive them. The cost of addressing these vulnerabilities grows immense, and what is revealed by recent events is that these costs are not merely technological.

The obligation to keep the adverse effects of the digital age has transformed the contest into one aimed arrow-like at human cognition. Numerous Defense Advanced Research Projects Agency (DARPA) programs search for ways to fill security vulnerabilities in the infrastructures of cyberspace.[71] One study considers whether the US would benefit more than its adversaries if fully homomorphic encryption were developed to the point of widespread use.[72] The authors' findings are highly equivocal about what would be an immensely costly intervention in digital infrastructure. At the same time, the co-evolution of these vulnerabilities with human cognitive vulnerabilities has made it impossible to quarantine people and whole societies from the increasingly sharp strategic contest. DARPA is also the home of a number of programs in which various aspects of the cognitive neurosciences are fully entangled with the strategic contest.[73] Exacerbating this problem is the reliance of the NSID community on the private sector for much of the data gathering and analytics. Marshall acknowledged this in 1999: "The DoD has little control over the pace and direction of the information revolution... (it) needs to manage a difficult transition from being a pioneer to being a leading user."[74]

The psychology and philosophy of cognition, which for centuries was primarily a theoretical question, has become an engineering question. The "cognitive revolution" in psychology, epistemology, and computing beginning in the 1950s[75] has in the past two decades branched into the closely related sciences of "cognitive neuroscience" and "cognitive engineering."[76] Today, these fields sit at the heart of strategic science and technology. DARPA's "Explainable Artificial Intelligence" (XAI) program is indicative of where the fields meet.[77] The race is on to transform advances in machine and deep learning into society-wide strategic assets.[78] For this, the field is endeavoring to make the human-machine interface a zone compatible with normal human tendencies. Machines able to render outputs, no matter how sophisticated, which cannot

mesh with human requirements such as the need for explanation and trust, will not deliver widespread applications.

XAI is aimed at building an "explanation interface" into AI systems, which deliver on this requirement via the inclusion of a causal reasoning module.[79] This need, therefore, to understand and model the "psychology of explanation" is at the heart of the cognitive sciences. For this, the mass data collection and analytics of the Silicon Valley Internet monopolies are invaluable. The relationship between these and other private sector entities and government agencies has been well documented.[80] In the 2017-18 financial year, hundreds of thousands of search warrants, subpoenas, court orders, and other legal requests were put to AT&T, Verizon, and Google by local, state, and federal government authorities in the US.[81] The relationship has its problems.[82] Nonetheless, as it progresses, the full scope of exploitable vulnerabilities in human cognition will be revealed to scientists, and their findings will be available to public and private entities with a myriad of motivations. As Robert McCreight warns:

> If the central goal is to manipulate human thought, emotions, and behaviour through a combination of psychopharmacological, biotechnical, and cybernetic activities and synergized systems to steer, influence, and shape thought and conduct – then we must be and remain alert to such potential goals and progress toward them to date.[83]

No one need posit any nefarious motivations on the behalf of researchers or the NSID community. The simple fact is that each technological epoch society traverses is in part characterized by the ways and means by which humans contend with one another. The human mind has never been fully insulated from this contest. Yet, more and more tools and techniques are becoming available for the exploitation of this space to unprecedented effect, and something of an arms race is accelerating.[84] In addition, the ethics of cognitive neuroscience have been acknowledged as woefully underdeveloped and in urgent need of public attention.[85] The cultivation and exploitation of human attention have become a lucrative enterprise for Silicon Valley monopolists at the same time that its secrets have become of compelling national security interest.[86]

Unfortunately, the confluence of the high economic and strategic value placed on the manipulation of human cognitive processes is having deleterious effects on social stability and the basic functionality of the polity in the US and elsewhere. Warnings from the late 1990s of the inherent uncertainty associated with highly complex information systems have been realized. Numerous challenging questions face the US polity at the same time as the functionality of the polity is frozen and social instability is a rising threat. How should the polity respond to the overwhelming monopoly power of the Silicon Valley giants?[87] What can be done about the widely despised attention-based Internet model that would not crash the value of the NASDAQ?[88] How can foreign interference be thwarted?[89] Does the promise of AI as a military-strategic asset mean the Internet primes are essentially beyond legislative control?[90]

These and many others are the most vexatious questions the US has faced in generations, at the same time its polity is experiencing extraordinary levels of dysfunction. Adversaries and

competitors with even a minimal interest in seeing the US remain dysfunctional, let alone enemies with an interest in system failure, need do little more than seek ways to exacerbate these internal tensions at a chosen time and place.[91] Russia did not need to invent the Internet, the World Wide Web (WWW), portable mobile computing, the attention-based business model, and social media. It has simply used these readily available instruments to cause cognitive chaos, operations which have employed perhaps a hundred operatives.[92] China has used the Internet to acquire troves of intellectual property illegally.[93] The underlying target of both states is the systemic trust which constitutes the sinews of functionality in open democratic societies.[94] This is a prime example of optionality, expertly leveraged.

For their parts, Russia and China have sought to keep features of the digital age useful to them and discard the adverse features. Since 1991, each has pursued a regime of networked and mobile force elements largely aimed at preventing US and allied dominance in the way of war and in strategic competition more generally. Under the anti-access, area denial (A2AD) rubric, the aim is to deny US and allied forces the unimpeded use of the air, sea, land, space, and cyberspace they require to prosecute high-tempo conventional operations.[95] These efforts are asymmetric, as China and Russia have no illusions about meeting US forces at their strongest point. Both have managed to maneuver beneath a line above which a conventional military confrontation with US forces would occur; Russia in the Ukraine and Syria, and China in the South China Sea, are pre-eminent examples. Disruption and denial of the EMS, space elements, and cyberspace are major components of the A2AD approach. US Multi-Domain Operations are geared specifically toward overcoming these challenges. It is, however, in the civilian domain where Russia and China have repurposed the digital age to their strategic advantage and exacerbated the vulnerabilities of US and allied systems.[96]

China is among the world's most connected digital societies, but the Chinese Communist Party (CCP) has pursued a path of tailored social and political control built into the way cyberspace works in China.[97] Its notorious social credit system, which applies the tools of machine learning to mass surveillance, is being tested in multiple provinces.[98] For the most part, it seems Chinese citizens do not harbor major objections to this level of government surveillance, and the CCP's efforts enjoy a level of social and political legitimacy.[99] China has its own indigenous versions of Internet search and social media platforms, through which citizens operate inside a largely invisible firewall, controlled by the CCP, that tailors their online experience.[100]

Russia's digital age is different than China's. Described by Paul and Matthews as a "firehose of falsehoods" model, Russia's approach is to undermine confidence, as broadly as possible, in any information, making the concept of truth contingent and transient.[101] Russia's polity, like all polities, copes with these circumstances in its own culturally and historically contingent way.[102] The ways in which American, Australian, Chinese, Russian, and all cultures are particular in their cognitive proclivities is a topic of great interest. Not covered here, understanding cultural cognitive differences and the foundational assumptions of polities, most importantly

our own assumptions, will be crucial in formulating effective responses to cognitive insecurity. What aspects of our cognitive orientation might be particularly vulnerable to manipulation in the digital age?

Acknowledge and Address the Gap

Militaries draw their mandate and resources exclusively from the state, but we should be mindful that this arrangement is only 372 years old. Human insecurity and conflict are tens of thousands of years old. The digital age has seen the state forfeit a number of its previously held monopolies in short shrift,[103] the consequences of which are only beginning to be felt. The revolution in public-key encryption of the 1970s severed the state's monopoly on privacy and secrecy.[104] Personal computing and the Internet swept away its monopoly on information flow, storage, and security. The capacity to influence has essentially been democratized. Quickly following in tow have been public expectations about the locus and identity of authority and legitimacy, which are fundamental pillars of statehood. Knowledge itself has been under attack for some time.[105] In some parts of the world, the state stands not alone but side-by-side with digital-savvy non-state entities, including criminal gangs, tribal and religious authorities, and corporate actors, in the provision of basic civil services.[106]

The privatization of security services in war zones has risen in the public's consciousness.[107] The financial industry is being disrupted by non-traditional lending and transaction services, and centralized monetary regimes look set for change as cryptographically secured digital currencies emerge to challenge national currencies.[108] There seem to be few enterprises of collective human life not touched by the shifting asymmetries of power enabled by the digital age, and the primary purposeful activities of the associated institutions are adapting. As mentioned in the introduction, the expectation that the NSID community accounts for the locus and source of societal responses to the insecurity of the digital age is widespread. But we have argued that the NSID community, with the military at the forefront, has responsibilities for those activities associated exclusively with operational IW. A category error has obfuscated the growing gap.

The needs of cognitive security in the digital age are of a different type. The digital age has changed society and the military, but the most important factor is how it has changed the relationship between the two. The question put by Builder in 1999 was to what extent the digital age would alter the primary purposeful activity of the military, its "enterprise."[109] Would it simply seek to apply new tools to an old enterprise, or would the new tools fundamentally change the enterprise, as was the case with mechanized war, nuclear weapons, and the opening of space in the 20th century? These changes took time to mature, and any answer to Builder's question remains pending. What seems undeniable is that the military enterprise in the digital age has changed significantly and unpredictably, and that these changes are in their infancy. The transformation continues, and the gap between the demand for and the supply of security products and services has widened while we await their maturation.

The NSID community is entangled in a complex and difficult transformation brought on by the digital age. Multiple and conflicting imperatives and motivations are in play, but the public sees only fragments of these tensions in debates over privacy and secrecy, surveillance and security, monopoly and democracy, and so on. Cognitive insecurity of the sort that has destabilized and disrupted American society since the 2016 election is a manifestation of the unpredictable nature of complexity, complexity both exacerbated so acutely by hyper-connectivity and turned into a quasi-extractive industry by Silicon Valley.[110] A growing number of experts are forwarding a view, however, that the needs of cognitive security for open societies in the digital age cannot be met by military enterprise alone.[111] In 1999, Builder presaged a greater burden for civil society:

> Defensive information warfare may turn out to be the distributed burden of society every bit as much as its military—where all who use the fruits of the information revolution, civilian or military, must look after their own protection.[112]

Clint Watts, a former FBI Special Agent who has worked for years countering radical extremism inside and outside official channels,[113] believes slow-to-adapt government institutions are not the answer when it comes to contending with digital information operations. Watts has advocated for the growth of online civilian armies of digital defenders—cyber-educated guerrillas able to detect, deny, and disrupt enemy incursions into the cognitive battle space.[114] In truth, a model of amateur online warriors, receiving implicit and deniable approval from government agencies, is one exploited by Russian and Chinese authorities for some time. Rand Waltzman, who created DARPA's Social Media in Strategic Communication program,[115] believes "the nature of interactions with the information environment are rapidly evolving and old models are becoming irrelevant faster than we can develop new ones. The result is uncertainty that leaves us exposed to dangerous influences without proper defences."[116] Waltzman advocates bringing together: "Cognitive science, computer science, engineering, social science, security, marketing, political campaigning, public policy, and psychology to develop a theoretical as well as an applied engineering methodology for managing the full spectrum of information environment security issues."[117]

Cognitive security is a unique challenge in that it traverses the security architecture of open societies, between policing criminal activity and countering the activities of malicious foreign agents. The reality is that these domains are unified at the digital machine/human interface, and so must be the response,[118] but the response is not merely a technological one. The institutional role of the military in the social fabric of open society has always extended beyond the battlefield. As a trusted social institution, and a resource of great depth, history, and stability, its role in pushing its values forward as the institutional life of open society is changing should not be overlooked.[119] We build trust side-by-side and bottom-up. Only by doing so can the fruits of the digital age be retained, and its dangers, flaws, and errors mitigated. Strategic gain in the digital age will depend on building this trust.

CONCLUSION

A good deal of skeptical caution should also be applied. The hubris which convinced many that the digital information age would supply a strategic *fait accompli* to US and allied competitors has been met sharply by unpredictable reality. In the same way, beliefs that advances in deep-learning AI and other data-driven tools and methods can be applied to the society-centric contest, to gain strategic advantage over the adversaries of open democratic societies, rely on dangerous assumptions.[120] For proponents of narrative warfare, the questions of narrative fratricide, blowback, and the unanticipated side effects of their interventions loom large. Can and should open democratic societies seek to manipulate the manipulators? Game the gamers? What are the implications of these measures, which are certain to create even more mass distrust, for the fabric of trust on which open society depends?[121] As Josh Kerbel puts it, could calls for states to engage in narrative warfare be an example of "activity masquerading as progress"?[122] What of the unintended consequences of that activity? Society-centric war is an attack on the sinews of trust that bind and facilitate open societies, enabled nowadays by the digital medium. Responses that risk the further erosion of the social fabric by gamifying societal functionality via the digital medium swallow that bait. The strategic task is great and requires a whole-of-society response: How to live freely and securely in the technological landscapes we have created, deployed, and scaled, and whose wisdom we now question.

NOTES

1. John Keegan, *A History Of Warfare* (Random House, 2011), xvi.
2. For excellent review of this discourse see Sean T. Lawson, *Nonlinear Science and Warfare: Chaos, Complexity and the U.S. Military in the Information Age* (Routledge, 2013); Sean Lawson, "Cold War Military Systems Science and the Emergence of a Nonlinear View of War in the US Military," *Cold War History* 11, no. 3 (August 1, 2011): 421-40, https://doi.org/10.1080/14682745.2010.494302.
3. For canonical overview see Manuel Castells, *The Information Age, Volumes 1-3: Economy, Society and Culture* (Wiley, 1999); Manuel Castells, "Materials for an Exploratory Theory of the Network Society," T*he British Journal of Sociology* 51, no. 1 (2000): 5-24.
4. Maryanne Kelton et al., "Australia, the Utility of Force and the Society-Centric Battlespace," *International Affairs,* May 28, 2019, https://doi.org/10.1093/ia/iiz080.
5. Joseph S. Nye, Jr., and William A. Owens, "America's Information Edge," *Foreign Affairs,* 1996, 20-36.
6. Notable exceptions included Barry D. Watts, *Clausewitzian Friction and Future War* (DIANE Publishing, 1996); Charles J. Dunlap, Jr., "21st-Century Land Warfare: Four Dangerous Myths," *Parameters,* Autumn 1997, https://ssi.armywarcollege.edu/pubs/Parameters/articles/97autumn/dunlap.htm.
7. Zalmay Khalilzad et al., *Strategic Appraisal: The Changing Role of Information in Warfare* (RAND Corporation, 1999), 22, http://www.rand.org/pubs/monograph_reports/MR1016.html.
8. Edward Luttwak, *Turbo-Capitalism: Winners and Losers in the Global Economy (*New York: HarperCollins Publishers, 1999).
9. Patrick E. Tyler, "U.S. Strategy Plan Calls for Ensuring No Rivals Develop," *The New York Times,* March 8, 1992, sec. World, http://www.nytimes.com/1992/03/08/world/us-strategy-plan-calls-for-insuring-no-rivals-develop.html.
10. Richard L. Kugler, "Dissuasion as a Strategic Concept" (Fort McNair, Washington, DC: National Defense University Institute for National Strategic Studies, 2002), http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA421905.
11. G. John Ikenberry, *America Unrivaled: The Future of the Balance of Power* (Cornell University Press, 2002).
12. Edward N. Luttwak, "From Geopolitics to Geo-Economics: Logic of Conflict, Grammar of Commerce," The National Interest, no. 20 (1990): 17-23; Richard Nixon, *Seize the Moment: America's Challenge in a One-Superpower World* (Simon and Schuster, 2013).
13. The September/October edition of *Foreign Affairs* is noteworthy on this topic, https://www.foreignaffairs.com/search?qs=september+october+1997.
14. US Intelligence Community, "Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution" (Office of the Director of National Intelligence, January 6, 2017), https://publicintelligence.net/odni-russian-election-operations/; Senate Select Committee on Intelligence, "The Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent U.S. Elections" (United States Senate, July 3, 2018), https://www.burr.senate.gov/imo/media/doc/SSCI%20ICA%20ASSESSMENT_FINALJULY3.pdf.
15. James R. Clapper and Trey Brown, *Facts and Fears: Hard Truths from a Life in Intelligence* (Penguin, 2018).
16. Michael V. Hayden, *The Assault on Intelligence: American National Security in an Age of Lies (*Penguin, 2018).
17. Martin C. Libicki, *Illuminating Tomorrow's War* (DIANE Publishing, 1999).
18. Martin C. Libicki, "Information War, Information Peace," *Journal of International Affairs* 51, no. 2 (1998): 411.
19. Khalilzad et al., *Strategic Appraisal: The Changing Role of Information in Warfare,* iii.
20. Libicki, 411-12.
21. Libicki, 411.
22. Khalilzad et al., *Strategic Appraisal: The Changing Role of Information in Warfare,* 21.
23. Khalilzad et al., 1-6.

NOTES

24. Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge University Press, 2007); Martin C. Libicki, "Cyberwar as a Confidence Game," *Strategic Studies Quarterly* 5 (2011), http://elastic.org/~fche/mirrors/www.cryptome.org/2013/07/cyber-war-racket-0012.pdf; John B. Sheldon, "Deciphering Cyberpower Strategic Purpose in Peace and War," *Strategic Studies Quarterly: SSQ; Maxwell Air Force Base* 5, no. 2 (Summer 2011): 95-112; John Arquilla, "Can Information Warfare Ever Be Just?" *Ethics and Information Technology; Dordrecht* 1, no. 3 (1999): 203-12; Dorothy Elizabeth Robling Denning, *Information Warfare and Security* (ACM Press, 1999); Roger C. Molander et al., *Strategic Information Warfare: A New Face of War* (Rand Corporation, 1996); Klaus Schwab, *The Fourth Industrial Revolution* (New York: Crown Business, 2017); Alvin Toffler and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Warner Books, 1994); Carmine Cicalese, "Redefining Information Operations," *Joint Force Quarterly/ National Defense University* 69 (April 2013); Frans P.B. Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd* (Routledge, 2007); D. McCarthy, *Power, Information Technology, and International Relations Theory: The Power and Politics of US Foreign Policy and the Internet* (Springer, 2015); Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (New York: Oxford University Press, 2015); Chris C. Demchak and Peter J. Dombrowski, "Rise of a Cybered Westphalian Age: The Coming Decades," in *The Global Politics of Science and Technology - Vol. 1,* Global Power Shift (Springer, Berlin, Heidelberg, 2014), 91-113, https://doi.org/10.1007/978-3-642-55007-2_5.
25. Laura Rosenberger and John Garnaut, "The Interference Operations from Putin's Kremlin and Xi's Communist Party: Forging a Joint Response," *The Asan Forum* (blog), May 8, 2018, http://www.theasanforum.org/the-interference-operations-from-putins-kremlin-and-xis-communist-party-forging-a-joint-response/; Thomas Mahnken, Ross Babbage, and Toshi Yoshihara, "Countering Comprehensive Coercion: Competitive Strategies Against Authoritarian Political Warfare" (Center for Strategic and Budgetary Assessments, May 2018), https://csbaonline.org/uploads/documents/Countering_Comprehensive_Coercion%2C_May_2018.pdf; James Scott and Drew Spaniel, *China's Espionage Dynasty: Economic Death by a Thousand Cuts* (CreateSpace Independent Publishing Platform, 2016); Jordan Robertson and Michael Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies," *Bloomberg* (blog), October 4, 2018, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies?srnd=businessweek-v2; James J. Wirtz, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy," in *Cyber War in Perspective: Russian Aggression Against Ukraine* (Tallinn: NATO CCD COE Publications, 2015); Senate Select Committee on Intelligence, "The Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent U.S. Elections"; Christopher Paul and Miriam Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model" (Santa Monica, California: RAND Corporation, 2016), https://www.rand.org/pubs/perspectives/PE198.html.
26. John Arquilla, "The Strategic Implications of Information Dominance" (Calhoun Institutional Archive of the Naval Postgraduate School, 1994); Martin C. Libicki, "The Convergence of Information Warfare," *Strategic Studies Quarterly*, Spring 2017, http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-11_Issue-1/Libicki.pdf; H.R. McMaster, "Crack in the Foundation: Defense Transformation and Underlying Assumption of Dominant Knowledge in Future War," *Center for Strategic Leadership, U.S. Army War College* S03, no. 3 (November 2003), http://www.au.af.mil/au/awc/awcgate/army-usawc/mcmaster_foundation.pdf; Alicia Wanless and Michael Berk, "The Strategic Communication Ricochet: Planning Ahead for Greater Resiliency," *The Strategy Bridge* (blog), March 7, 2018, https://thestrategybridge-org.cdn.ampproject.org/c/s/thestrategybridge.org/the-bridge/2018/3/7/the-strategic-communication-ricochet-planning-ahead-for-greater-resiliency?format=amp; David S. Alberts et al., *Understanding Information Age Warfare*, n.d.; Emily Goldman and Thomas G. Mahnken, *The Information Revolution in Military Affairs in Asia* (Palgrave Macmillan, 2004); Peter Hall and Robert Wylie, "The Revolution in Military Affairs and Australia's Defense Industry Base, 1996-2006," *Security Challenges Volume 4, Number 4 (Summer 2008), 57-80*, accessed February 2, 2015, http://www.securitychallenges.org.au/ArticlePages/vol4no4HallandWylie.html; Wang Xiangsui and Qiao Liang, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999); Valery Gerasimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Military Review*, February 2016, http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf.
27. Arquilla, "The Strategic Implications of Information Dominance"; John Arquilla and David Ronfeldt, "Cyberwar Is Coming!" *Comparative Strategy* 12, no. 2 (April 1, 1993): 141-65, https://doi.org/10.1080/01495939308402915; John Arquilla et al., *The Emergence of Noopolitik: Toward An American Information Strategy* (Rand Corporation, 1999); Martin Libicki, "The Emerging Primacy of Information," *Orbis* 40, no. 2 (1996): 261-274.
28. Edward A. Smith, Jr., "Effects-Based Operations," *Security Challenges* 2, no. 1 (2006): 43, https://www.regionalsecurity.org.au/Resources/Files/vol2no1Smith.pdf.

NOTES

29. Edward A. Smith, Jr., *Effects Based Operations: Applying Network Centric Warfare to Peace, Crisis, and War* (DOD-CCRP, 2002).
30. Ariel E. Levite and Jonathan (Yoni) Shimshoni, "The Strategic Challenge of Society-Centric Warfare," *Survival* 60, no. 6 (November 2, 2018): 91-118, https://doi.org/10.1080/00396338.2018.1542806.
31. Smith Jr., "Effects-Based Operations," 43.
32. Timothy L. Thomas, *Dragon Bytes: Chinese Information-War Theory and Practice*, 1st edition (Foreign Military Studies Office, 2004), https://babel.hathitrust.org/cgi/pt?id=uiug.30112065967041;view=1up;seq=37; Wirtz, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy"; Fiona Hill and Clifford G. Gaddy, *Mr. Putin: Operative in the Kremlin* (Brookings Institution Press, 2015); Peter Pomerantsev, "The Hidden Author of Putinism," *The Atlantic*, November 7, 2014, https://www.theatlantic.com/international/archive/2014/11/hidden-author-putinism-russia-vladislav-surkov/382489/; Scott and Spaniel, *China's Espionage Dynasty*.
33. Emile Simpson, *War From the Ground Up: Twenty-First Century Combat as Politics* (Oxford University Press, 2012); Richard D'Aveni, "Waking Up to the New Era of Hypercompetition," *Washington Quarterly* 21 (March 1, 1998): 183–95, https://doi.org/10.1080/01636609809550302.
34. Jonathan D. Moreno, *Mind Wars: Brain Science and the Military in the Twenty-First Century* (Bellevue Literary Press, 2012); James Giordano, ed., *Neurotechnology in National Security and Defense: Practical Considerations, Neuroethical Concerns* (CRC Press, 2014).
35. General David L. Goldfein, "Air Force Association Remarks" (September 19, 2017), http://www.af.mil/Portals/1/documents/csaf/CSAF_AFA_2017%20Air_Space_and_Cyber_Symposium.pdf; Vincent R. Stewart, DoDIIS Worldwide Conference Opening Remarks (Atlanta, Georgia, 2017), https://vimeo.com/206476865; *Exploring Cognitive Warfare*, Over the Horizon, n.d., https://othjournal.com/2017/11/08/oth-podcast-4-exploring-cognitive-warfare/; Tyler Quinn and Von Lambert, "Musings on the Prominence of Informational Effects in the Operational Art," Grounded Curiosity, May 21, 2018, https://groundedcuriosity.com/musings-on-the-prominence-of-informational-effects-in-the-operational-art/; John Michael Fabry, "Information Warfare: Expanding the Paradigm" (Ph.D., Rutgers The State University of New Jersey - New Brunswick, 1998), https://search.proquest.com/docview/304453551/abstract/1D00BD1F4AA1468FPQ/1; Rand Waltzman, "A Center for Cognitive Security - Draft Proposal," *IPA Information Professionals Association.* (blog), April 18, 2017, https://information-professionals.org/a-center-for-cognitive-security-draft-proposal/; Kimberly Underwood, "Cognitive Warfare Will Be Deciding Factor in Battle," SIGNAL Magazine, August 15, 2017, https://www.afcea.org/content/cognitive-warfare-will-be-deciding-factor-battle; Emily Bienvenue, Zac Rogers, and Sian Troath, "Cognitive Warfare: The Fight We've Got," The Cove, September 19, 2018, https://www.cove.org.au/adaptation/article-cognitive-warfare-the-fight-weve-got/; George Popp, Sarah Canna, and N. Peterson, eds., "From Control to Influence? A View of – and Vision for – the Future" (10th Annual Multilayer Assessment (SMA) Conference, Joint Base Andrews, 2017), http://nsiteam.com/social/wp-content/uploads/2017/06/U_Final_SMA-Conference-Proceedings-25-26-April-2017.pdf; Rand Waltzman, "The Weaponization of Information: The Need for Cognitive Security," § Senate Armed Services Committee, Subcommittee on Cybersecurity (2017), https://www.rand.org/pubs/testimonies/CT473.html.
36. Goldfein, "Air Force Association Remarks."
37. Stewart, DoDIIS Worldwide Conference Opening Remarks.
38. Lauren Elkins, "The 6th Warfighting Domain," OTH, November 5, 2019, https://othjournal.com/2019/11/05/the-6th-warfighting-domain/.
39. Waltzman, "A Center for Cognitive Security – Draft Proposal"; Waltzman, The Weaponization of Information: The Need for Cognitive Security.
40. "Martin C. Libicki, "What Is Information Warfare?" (National Defense University: Center for Advanced Concepts and Technology, Institute for National Strategic Studies, August 1995), x, http://www.dtic.mil/dtic/tr/fulltext/u2/a367662.pdf.
41. Office of the Chairman of the Joint Chiefs of Staff, "Joint Information Warfare Policy" (Washington, DC: Chairman of the Joint Chiefs of Staff Instruction 3210.01, January 2, 1996).
42. Libicki, "What Is Information Warfare?" x.
43. Toffler and Toffler, *War and Anti-War.*

NOTES

44. David S. Alberts, "The Future of Command and Control with DBK," in *Dominant Battlespace Knowledge* (National Defense University, 1995); Paul Bracken, "The Significance of DBK," in *Dominant Battlespace Knowledge* (National Defense University, 1995); Martin Libicki, "DBK and Its Consequences," in *Dominant Battlespace Knowledge* (National Defense University, 1995), http://www.dodccrp.org/files/Libicki_Dominant.pdf.
45. Libicki, "The Convergence of Information Warfare."
46. U.S. Army, "Army Special Operations Forces Unconventional Warfare," September 30, 2008, https://file.wikileaks.org/file/us-fm3-05-130.pdf; U.S. Marine Corps Combat Development Command and U.S. Special Operations Command Center for Knowledge and Futures, "Multi-Service Concept for Irregular Warfare," August 2006, https://file.wikileaks.org/file/us-iw-multi-service-2006.pdf; John Strand, *Offensive Countermeasures: The Art of Active Defense*, 2nd ed. (John Strand Paul Asadoorian, 2017); Wyatt Hoffman and Ariel E. Levite, "Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?" (Carnegie Endowment for International Peace, June 14, 2017), http://carnegieendowment.org/2017/06/14/private-sector-cyber-defense-can-active-measures-help-stabilize-cyberspace-pub-71236; James Lewis, "Rethinking Cybersecurity: Strategy, Mass Effects, and States," CSIS Technology Program (CSIS, January 2018).
47. Libicki, "The Convergence of Information Warfare."
48. Robert Work and Shawn Brimley, *20YY: Preparing for War in the Robotic Age* (Washington, DC: Center for a New American Security, 2014), 17.
49. See biographies of Boyd's life and work, Osinga, *Science, Strategy and War*; Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War* (Hachette UK, 2002); and Boyd's unpublished work accessible at John R. Boyd, "Patterns of Conflict," *A Discourse on Winning and Losing, (unpublished manuscript)*, 1987, http://dnipogo.org/john-r-boyd/; John R. Boyd, "Destruction and Creation," *A Discourse on Winning and Losing, (Unpublished Manuscript)*, 1987, http://dnipogo.org/john-r-boyd/.
50. Ian Brown, "Opening the Loop: A Look inside the Mind of John Boyd," *Marine Corps Gazette*, June 2015, https://www.mcafdn.org/gazette/2015/06/opening-loop.
51. Osinga, *Science, Strategy and War,* chaps. 4-5.
52. Coram, *Boyd*, 120.
53. Explored most prominently over three decades in the work of Donald D. Hoffman, *The Case Against Reality: How Evolution Hid the Truth from Our Eyes* (Penguin UK, 2019).
54. Popper introduced the assertion that scientific knowledge can only progress through falsification. Unspecified and unassigned items of knowledge about the world are by definition unfalsifiable and do not count as knowledge under this formulation. Operational IW is Popperian in the sense that it involves making discrete claims about narrow aspects of the world which are falsifiable. Karl Popper, *The Logic of Scientific Discovery* (Routledge, 2005); Karl Popper, *Conjectures and Refutations: The Growth of Scientific Knowledge* (Routledge, 2014).
55. Polanyi and Kuhn offer responses to Popper which support the view that falsifiable claims alone cannot account for the growth of knowledge. Michael Polanyi, *The Tacit Dimension* (University of Chicago Press, 2009); Thomas S. Kuhn, *The Structure of Scientific Revolutions: 50th Anniversary Edition* (University of Chicago Press, 2012).
56. Manuel Castells, *The Information Age*, Volumes 1-3: Economy, *Society and Culture* (Wiley, 1999); Joshua Cooper Ramo, *The Seventh Sense: Power, Fortune, and Survival in the Age of Networks* (New York: Little, Brown and Company, 2016); David S. Alberts, John J. Garstka, and Frederick P. Stein, Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd ed. (DoD C4ISR Cooperative Research Program, 2000).
57. Paul T. Mitchell, *Network Centric Warfare and Coalition Operations: The New Military Operating System* (Routledge, 2009); Martin C. Libicki, *Illuminating Tomorrow's War* (DIANE Publishing, 1999); Martin C. Libicki and Stuart E. Johnson, eds., "Dominant Battlespace Knowledge" (National Defense University, October 1995), http://www.dodccrp.org/files/Libicki_Dominant.pdf.
58. Jeffrey M. Reilly, "Multidomain Operations: A Subtle but Significant Transition in Military Thought," *Air & Space Power Journal* 30, no. 1 (2016): 61; Maj Sean A. Atkins, USAF, "Multidomain Observing and Orienting: ISR to Meet the Emerging Battlespace," *Air & Space Power Journal,* Fall 2018, https://www.airuniversity.af.mil/ASPJ/; Albert Palazzo, "Multi-Domain Battle: The Echo of the Past," *The Strategy Bridge* (blog), October 11, 2017, https://thestrategybridge.org/the-bridge/2017/10/11/multi-domain-battle-the-echo-of-the-past.

NOTES

59. C. Kopp, "Fifteen Constraints on the Capability of High-Capacity Mobile Military Networked Systems," July 2007, http://search.informit.com.au/documentSummary;dn=090370892216290;res=IELENG; Paul T. Mitchell, "Freedom and Control: Networks in Military Environments," *The Adelphi Papers* 46, no. 385 (December 1, 2006): 27-44; Stanley A. McChrystal, "It Takes a Network," *Foreign Policy* (blog), accessed November 16, 2015, https://foreignpolicy.com/2011/02/21/it-takes-a-network/; Gary A. Whitted and Captain Mary E. Just, "Advanced Collaborative Technologies Supporting the 21st Century Warfighter in a Network Centric Environment" (Proceedings of the 2005 International Symposium on Collaborative Technologies and Systems, IEEE Conference Publications, May 2005).
60. Nate Freier et al., "Game On or Game Over: Hypercompetition and Military Advantage," US Army War College War Room, May 22, 2018, https://warroom.armywarcollege.edu/articles/the-new-defense-normal-nine-fundamentals-of-hypercompetition/; Mari Eder, "The Information Apocalypse… Is Already Here," US Army War College War Room, August 22, 2018, https://warroom.armywarcollege.edu/articles/information-apocalypse/; Hezekiah Winter, "Total Disinformation Warfare," Hacker Noon, June 9, 2018, https://hackernoon.com/on-russian-and-washington-propaganda-c95f553a6776.
61. Peter Layton, "Fifth Generation Warfare: An Evolving Technical Dimension of War," Over the Horizon, July 31, 2017, https://overthehorizonmdos.com/2017/07/31/5th-gen-warfare/; Peter Layton, *Algorithmic Warfare Applying Artificial Intelligence to Warfighting* (Air Power Development Centre, 2018), http://airpower.airforce.gov.au/APDC/media/PDF-Files/Contemporary%20AirPower/AP33-Algorithmic-Warfare-Applying-Artificial-Intelligence-to-Warfighting.pdf; Peter Layton, "America's Air Power Revolution," *Defense Today*, March 2018, https://drive.google.com/file/d/1On7yP-dPtGx4f4dDVb2g5G5zxv2OkeZNL/view.
62. Libicki and Johnson, "Dominant Battlespace Knowledge," v.
63. Libicki and Johnson, 33.
64. Libicki and Johnson, 19.
65. Arquilla et al., *The Emergence of Noopolitik*; Arquilla, "The Strategic Implications of Information Dominance."
66. Khalilzad et al., *Strategic Appraisal: The Changing Role of Information in Warfare*, 1, emphasis added.
67. Col. Michael W. Pietrucha, "The Search for the Technological Silver Bullet To Win Wars," War on the Rocks, accessed September 2, 2015, http://warontherocks.com/2015/08/the-search-for-the-technological-silver-bullet-to-win-wars/.
68. Christian Davenport, "Efforts Underway to Improve Pentagon's Procurement System," *The Washington Post*, December 1, 2014, https://www.washingtonpost.com/business/economy/why-the-pentagon-spent-46b-on-12-weapon-programs-it-never-finished/2014/12/01/c1787814-74f7-11e4-9d9b-86d397daad27_story.html; Mike Pietrucha, "The Phantom Menace: When Threat Capabilities Are Made Up," War on the Rocks, September 21, 2016, http://warontherocks.com/2016/09/the-phantom-menace-when-threat-capabilities-are-made-up/.
69. Reilly, "Multidomain Operations: A Subtle but Significant Transition in Military Thought," 67.
70. Nassim Nicholas Taleb, *Incerto: Antifragile, the Black Swan, Fooled by Randomness, the Bed of Procrustes* (Random House Publishing Group, 2016).
71. Brad D. Williams, "DARPA Moves to Innovate Cyber Intel Capability with Real-Time Threat Visualization," Fifth Domain | Cyber, June 23, 2017, http://fifthdomain.com/2017/06/23/darpa-moves-to-innovate-cyber-intel-capability-with-real-time-threat-visualization/; DARPA, "DARPA Seeks More Robust Military Wireless Networks," DARPA, March 18, 2013, https://www.darpa.mil/news-events/2013-03-18; Nicole Blake Johnson, "DARPA's Cyber Antidote," *FedTech*, June 3, 2014, https://fedtechmagazine.com/article/2014/06/darpas-cyber-antidote; John Launchbury, "PROgramming Computation on EncryptEd Data (PROCEED)," DARPA, accessed April 10, 2017, http://www.darpa.mil/program/programming-computation-on-encrypted-data; Martin C. Libicki et al., "Ramifications of DARPA's Programming Computation on Encrypted Data Program" (National Defense Research Institute: RAND Corporation, 2014), http://www.rand.org/content/dam/rand/pubs/research_reports/RR500/RR567/RAND_RR567.pdf.
72. Libicki et al., "Ramifications of DARPA's Programming Computation on Encrypted Data Program."
73. Jonathan D. Moreno, "DARPA on Your Mind," Cerebrum, October 1, 2004, http://www.dana.org/Cerebrum/Default.aspx?id=39170; Joshua Elliot, "Active Social Engineering Defense (ASED)," DARPA, n.d., https://www.darpa.mil/program/active-social-engineering-defense; Justin Sanchez, "Narrative Networks," DARPA, n.d., https://www.darpa.mil/program/narrative-networks; DARPA, "Social Media in Strategic Communication (SMISC)," DARPA, n.d., https://www.darpa.mil/program/social-media-in-strategic-communication; DARPA, "Social Systems," DARPA, n.d., https://www.darpa.mil/about-us/dso-social-systems; Matthew Hepburn, "Strategic Social Interaction Modules (SSIM)," DARPA, n.d., https://www.darpa.mil/program/strategic-social-interaction-modules; Justin Sanchez, "Systems-Based Neurotechnology for Emerging Therapies (SUBNETS)," DARPA, n.d., https://www.darpa.mil/program/systems-based-neurotechnology-for-emerging-therapies.

NOTES

74. Khalilzad et al., *Strategic Appraisal: The Changing Role of Information in Warfare,* 2.
75. Howard E. Gardner, *The Mind's New Science: A History Of The Cognitive Revolution* (Hachette UK, 2008); Norbert Wiener, *The Human Use Of Human Beings: Cybernetics And Society* (Hachette UK, 1988); Gilbert Ryle, *The Concept of Mind: 60th Anniversary Edition* (Routledge, 2009); Gregory Bateson, *Mind and Nature: A Necessary Unity* (Hampton Press, 2002).
76. John T. Wixted and John Serences, eds., *Stevens' Handbook of Experimental Psychology and Cognitive Neuroscience, Sensation, Perception, and Attention*, 4th ed. (John Wiley & Sons, 2018); Johan Wagemans, ed., *The Oxford Handbook of Perceptual Organization* (OUP Oxford, 2015); Mica Endsley et al., "Cognitive Engineering and Decision Making: An Overview and Future Course," *Journal of Cognitive Engineering and Decision Making* 1 (March 1, 2007): 1-21, https://doi.org/10.1177/155534340700100101.
77. David Gunning, "Explainable Artificial Intelligence (XAI)," DARPA, n.d., https://www.darpa.mil/program/explainable-artificial-intelligence.
78. Cliff Kuang, "Can A.I. Be Taught to Explain Itself?" *The New York Times,* November 21, 2017, sec. Magazine, https://www.nytimes.com/2017/11/21/magazine/can-ai-be-taught-to-explain-itself.html; Ariel Bleicher, "Demystifying the Black Box That Is AI," *Scientific American,* August 9, 2017, https://www.scientificamerican.com/article/demystifying-the-black-box-that-is-ai/; Paul Voosen, "How AI Detectives Are Cracking Open the Black Box of Deep Learning," Science | AAAS, July 5, 2017, https://www.sciencemag.org/news/2017/07/how-ai-detectives-are-cracking-open-black-box-deep-learning; Sara Castellanos and Steven Norton, "Inside Darpa's Push to Make Artificial Intelligence Explain Itself," WSJ (blog), August 10, 2017, https://blogs.wsj.com/cio/2017/08/10/inside-darpas-push-to-make-artificial-intelligence-explain-itself/; Will Knight, "The Dark Secret at the Heart of AI," *MIT Technology Review,* April 11, 2017, https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/.
79. Judea Pearl and Dana Mackenzie, *The Book of Why: The New Science of Cause and Effect* (Penguin UK, 2018).
80. MDDS Working Group, "Call for Absracts for Massive Digital Data Systems," November 3, 1993, https://groups.google.com/forum/#!topic/mail.cypherpunks/4CDiW59hS88; D. Parkins, "Regulating the Internet Giants: The World's Most Valuable Resource Is No Longer Oil, but Data," *The Economist* 413 (May 6, 2017), https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource; Giovanni Navarria, Nick Couldry, and Rachell Li, "The Price of Connection: 'Surveillance Capitalism,'" The Conversation, September 23, 2016, http://theconversation.com/the-price-of-connection-surveillance-capitalism-64124; Bruce Schneier, "The Public/Private Surveillance Partnership," *Schneier on Security* (blog), August 5, 2013, https://www.schneier.com/blog/archives/2013/08/the_publicpriva_1.html; Bruce Schneier, "Surveillance as a Business Model," *Schneier on Security* (blog), November 25, 2013, https://www.schneier.com/blog/archives/2013/11/surveillance_as_1.html; Jeff Nesbit, "Google's True Origin Partly Lies in CIA and NSA Research Grants for Mass Surveillance," *Quartz (*blog), December 8, 2017, https://qz.com/1145669/googles-true-origin-partly-lies-in-cia-and-nsa-research-grants-for-mass-surveillance/.
81. AT&T, "Transparency Report," accessed October 24, 2018, http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html; Google, "Transparency Report," Google, accessed October 25, 2018, https://transparencyreport.google.com/user-data/overview?user_requests_report_period=authority:US; Verizon, "U.S. Report," Transparency Report, accessed October 24, 2018, https://www.verizon.com/about/portal/transparency-report/us-report/.
82. Scott Shane and Daisuke Wakabayashi, "'The Business of War': Google Employees Protest Work for the Pentagon," *The New York Times,* April 4, 2018, sec. Technology, https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html; David Taylor, "Big Tech's Double Trouble: Political Heat from Trump and the Left May Signal Reckoning Ahead," *The Guardian,* September 2, 2018, sec. Technology, https://www.theguardian.com/technology/2018/sep/02/big-techs-double-trouble-bipartisan-criticism-may-signal-a-reckoning-ahead; Cate Cadell, "Facebook Plans Innovation Hub in China despite Tightening Censorship," *Reuters,* July 24, 2018, https://www.reuters.com/article/us-china-facebook-subsidiary/facebook-sets-up-subsidiary-in-china-filing-idUSKBN1KE1JF; Kate Conger, "Google Employees Resign In Protest Against Pentagon Contract," *Gizmodo* (blog), May 15, 2018, https://www.gizmodo.com.au/2018/05/google-employees-resign-in-protest-against-pentagon-contract/; John Naughton, "Wanted in the Digital Monopoly Age – Powers to Curb the Hold of Online Giants," *The Guardian,* September 16, 2018, sec. Opinion, https://www.theguardian.com/commentisfree/2018/sep/16/wanted-in-digital-monopoly-age-powers-to-curb-online-giants.
83. Robert McCreight, "Brain Brinksmanship: Devising Neuroweapons Looking at Battlespace, Doctrine, and Strategy," in *Neurotechnology in National Security and Defense: Practical Considerations, Neuroethical Concerns* (CRC Press, 2015), 118.
84. McCreight, "Brain Brinksmanship: Devising Neuroweapons Looking at Battlespace, Doctrine, and Strategy."

NOTES

85. Giordano, *Neurotechnology in National Security and Defense*; James J. Giordano and Bert Gordijn, *Scientific and Philosophical Perspectives in Neuroethics* (Cambridge University Press, 2010).
86. Zac Rogers, "The Geopolitics of Surveillance Capitalism," *Chesterfield Strategy* (blog), September 16, 2019, https://chesterfieldstrategy.com/2019/09/16/the-geopolitics-of-surveillance-capitalism/.
87. Martin Moore and Damian Tambini, *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple* (Oxford University Press, 2018); Naughton, "Wanted in the Digital Monopoly Age – Powers to Curb the Hold of Online Giants."
88. Roger McNamee, "How to Fix Facebook—Before It Fixes Us," *Washington Monthly*, January 7, 2018, https://washingtonmonthly.com/magazine/january-february-march-2018/how-to-fix-facebook-before-it-fixes-us/; Nikhil Sonnad, "Everything Bad about Facebook Is Bad for the Same Reason," *Quartz* (blog), July 30, 2018, https://qz.com/1342757/everything-bad-about-facebook-is-bad-for-the-same-reason/.
89. Molly K. McKew, "Searching for a Stronghold in the Fight Against Disinformation," Centre for International Governance Innovation, June 4, 2018, https://www.cigionline.org/articles/searching-stronghold-fight-against-disinformation; Molly K. Mckew, "How Twitter Bots and Trump Fans Made #ReleaseTheMemo Go Viral," *POLITICO Magazine,* February 4, 2018, http://politi.co/2BSfTQ7; Clint Watts, *Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News* (HarperCollins, 2018).
90. Casey Newton, "Congress Just Showed Us What Comprehensive Regulation of Facebook Would Look Like," The Verge, July 31, 2018, https://www.theverge.com/2018/7/31/17632858/facebook-regulation-mark-warner-policy-paper-congress; Lina M. Khan, "Amazon's Antitrust Paradox," *The Yale Law Journal* 126, no. 3 (January 2017): 710-805; Taylor, "Big Tech's Double Trouble."
91. Adam Goldman, "Justice Dept. Accuses Russians of Interfering in Midterm Elections," *The New York Times*, October 20, 2018, sec. U.S., https://www.nytimes.com/2018/10/19/us/politics/russia-interference-midterm-elections.html.
92. Scott Shane and Mark Mazzetti, "The Plot to Subvert an Election: Unraveling the Russia Story So Far," *The New York Times*, September 20, 2018, https://www.nytimes.com/interactive/2018/09/20/us/politics/russia-interference-election-trump-clinton.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer.
93. Scott and Spaniel, *China's Espionage Dynasty.*
94. Ian Brown, "Imagining a Cyber Surprise: How Might China Use Stolen OPM Records to Target Trust?" War on the Rocks, May 22, 2018, https://warontherocks.com/2018/05/imagining-a-cyber-surprise-how-might-china-use-stolen-opm-records-to-target-trust/; Neal A. Pollard, Adam Segal, and Matthew G. Devost, "Trust War: Dangerous Trends in Cyber Conflict," War on the Rocks, January 16, 2018, https://warontherocks.com/2018/01/trust-war-dangerous-trends-cyber-conflict/; Rachel Botsman, *Who Can You Trust? How Technology Brought Us Together – and Why It Could Drive Us Apart* (Penguin UK, 2017).
95. Dmitri Trenin, "The Revival of the Russian Military: How Moscow Reloaded," F*oreign Affairs*, June 2016, https://www.foreignaffairs.com/articles/russia-fsu/2016-04-18/revival-russian-military; Mark Galeotti, "Heavy Metal Diplomacy: Russia's Political Use of Its Military in Europe since 2014" (European Council on Foriegn Relations, December 19, 2016), https://www.ecfr.eu/page/-/Heavy_Metal_Diplomacy_Final_2.pdf; Department of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2016," 2016, http://www.defense.gov/Portals/1/Documents/pubs/2016%20China%20Military%20Power%20Report.pdf.
96. Nance, *The Plot to Destroy Democracy*; Scott and Spaniel, *China's Espionage Dynasty;* Robertson and Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies"; Wirtz, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy."
97. Margaret E. Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall* (Princeton University Press, 2018).
98. Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras," *The New York Times,* October 15, 2018, sec. Business Day, https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.
99. Simina Mistreanu, "China Is Implementing a Massive Plan to Rank Its Citizens, and Many of Them Want In," *Foreign Policy*, April 3, 2018, https://foreignpolicy.com/2018/04/03/life-inside-chinas-social-credit-laboratory/.
100. Tiffany Li, "Opinion | China's Influence on Digital Privacy Could Be Global," *The Washington Post*, August 7, 2018, https://www.washingtonpost.com/news/theworldpost/wp/2018/08/07/china-privacy/.
101. Paul and Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model."
102. Pomerantsev, *Nothing Is True and Everything Is Possible.*

NOTES

103. Jessica T. Mathews, "Power Shift," *Foreign Affairs*, February 1997, https://www.foreignaffairs.com/authors/jessica-t-mathews.
104. Steven Levy, *Crypto: How the Code Rebels Beat the Government - Saving Privacy in the Digital Age* (Penguin, 2001).
105. Terry Wagner, "Expertise and Disbelief: Post-1945 American Attitudes Toward the Authority of Knowledge" (LSU Doctoral Dissertation, 2015), http://digitalcommons.lsu.edu/cgi/viewcontent.cgi?article=2975&context=gradschool_dissertations; Jennifer Kavanagh and Michael D. Rich, "Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life" (Santa Monica, CA: RAND Corporation, 2018), https://www.rand.org/pubs/research_reports/RR2314.html?adbsc=social_TruthDecay_20180619_24130011&adbid=641487755088707174 4&adbpl=li&adbpr=165654; Jonathan D. Moreno, *The Body Politic: The Battle Over Science in America* (Bellevue Literary Press, 2011).
106. Nils Gilman, "The Twin Insurgency," T*he American Interest* (blog), June 15, 2014, https://www.the-american-interest.com/2014/06/15/the-twin-insurgency/.
107. P.W. Singer, *Corporate Warriors: The Rise of the Privatized Military Industry* (Cornell University Press, 2011); Lindsey Cameron and Vincent Chetail, *Privatizing War: Private Military and Security Companies Under Public International Law* (Cambridge University Press, 2013).
108. Benjamin J. Cohen, The Future of Money (Princeton University Press, 2004); Zac Rogers, "Blockchain and the State: Vehicle or Vice?" *Australian Quarterly*, March 2018.
109. Khalilzad et al., *Strategic Appraisal: The Changing Role of Information in Warfare.*
110. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2019).
111. Katherine Mansted, "Activating People Power to Counter Foreign Interference and Coercion," Policy Options Paper (Canberra, ACT Australia: National Security College, ANU, December 2019), https://nsc.crawford.anu.edu.au/sites/default/files/publication/nsc_crawford_anu_edu_au/2019-12/pop_activating_people_power.pdf.
112. Khalilzad et al., *Strategic Appraisal: The Changing Role of Information in Warfare,* 36.
113. Clint Watts, "How About Some Unconventional Warfare? Thoughts On Countering ISIL," War on the Rocks, October 20, 2014, https://warontherocks.com/2014/10/how-about-some-unconventional-warfare-thoughts-on-countering-isil/; Clint Watts, "Advice for France in Its 'War on Terror,'" War on the Rocks, January 27, 2015, https://warontherocks.com/2015/01/advice-for-france-in-its-war-on-terror/; Clint Watts, "The Islamic State in Europe: Terrorists Without Borders, Counterterrorists With All Borders," War on the Rocks, March 29, 2016, https://warontherocks.com/2016/03/the-islamic-state-in-europe-terrorists-without-borders-counterterrorists-with-all-borders/.
114. Watts, *Messing with the Enemy.*
115. DARPA, "Social Media in Strategic Communication (SMISC)."
116. Waltzman, "A Center for Cognitive Security – Draft Proposal."
117. Waltzman.
118. See Reeder and Barnsby, "A Legal Framework Enhancing Cybersecurity through Public-Private Partnership," *The Cyber Defense Review*, Fall 2020, 31-45.
119. Emily Bienvenue and Zac Rogers, "Strategic Army: Developing Trust in the Shifting Strategic Landscape," *Joint Force Quarterly* 95 (November 2019): 4-14.
120. Zac Rogers, "158. In the Cognitive War – The Weapon Is You!" *Mad Scientist Laboratory* (blog), July 1, 2019, https://madsciblog.tradoc.army.mil/158-in-the-cognitive-war-the-weapon-is-you/.
121. Emily Bienvenue, Zac Rogers, and Sian Troath, "Trust as a Strategic Resource for the Defence of Australia," The Cove, October 29, 2018, https://www.cove.org.au/war-room/article-trust-as-a-strategic-resource-for-the-defence-of-australia/.
122. Josh Kerbel, "Coming to Terms with Anticipatory Intelligence," War on the Rocks, August 13, 2019, https://warontherocks.com/2019/08/coming-to-terms-with-anticipatory-intelligence/.

Digital Authoritarianism and Implications for US National Security

Justin Sherman

ABSTRACT

Digital authoritarianism, or the use of digital technologies to enhance or enable authoritarian governance, has received much attention due to its implications for human rights and global democracy. Yet, often overlooked are the implications of digital authoritarianism for US national security. This article explores the ways in which digital authoritarianism exposes US national security to risk on three fronts: consolidation of power in authoritarian regimes; increased incentives for authoritarians to promote diffusion of surveillance technologies; and potential insulation against foreign cyber attacks and lowered disincentives for authoritarians to conduct destabilizing cyber operations on the global Internet.

The US national security community increasingly is observing a phenomenon that for years has captured the interest of select academics, policy wonks, and human rights activists: "digital authoritarianism," where undemocratic regimes routinely use digital tools to enhance or enable authoritarian governing practices.[1] While definitions of digital authoritarianism are sparse[2]—and terminology remains disputed[3]—used here it refers to such practices as pervasive Internet surveillance and the exercise of tight control over online information flows within a country's borders. The Chinese and Russian governments have been the leading recipients of this "digital authoritarian" label, as they build out variously undemocratic practices, such as online censorship, using digital technologies.

Digital authoritarianism obviously impacts democracy and human rights. Controlling information flows within a country's borders, for instance, can quite effectively enable a government to crack down on anti-regime speech, or suppress the online organization of political dissidents. Perhaps less intuitively, the impacts of digital authoritarianism extend beyond human rights and democracy, to include the global economy and US national security. This article focuses on the last of these categories of implications—analyzing why

© 2021 Justin Sherman

Justin Sherman is a nonresident fellow at the Atlantic Council's Cyber Statecraft Initiative, a research fellow at the Tech, Law & Security Program at American University Washington College of Law, and a contributor at *WIRED* Magazine. He was previously a cybersecurity policy fellow at New America and a fellow at Duke Law School's Center on Law & Technology.

digital authoritarianism goes beyond human rights and democracy implications (which, normatively speaking, is already reason for concern), and can also undermine US national security and change the landscape of military and intelligence cyberspace operations.

First, digital authoritarianism allows authoritarian regimes to consolidate power—many of which already pose national security risks to the US, such as through malicious cyber activity and nuclear weapons. Second, digital authoritarianism may encourage certain technologically sophisticated governments, such as in China and Russia, to further encourage the global diffusion of tools and knowledge for digital surveillance. Third, digital authoritarianism, in the form of Internet isolation, could potentially insulate certain countries from foreign cyber attacks, thereby degrading disincentives to those that might create digital chaos on the global Internet. These main risks are addressed below.

1. AUTHORITARIANS CONSOLIDATING POWER

Digital authoritarianism, at its core, is a mechanism for exerting increased, unchecked control over one's population through digital technologies. Censorship, device hacking, and mass surveillance are all on the table. In this way, digital authoritarianism facilitates power consolidation—ensuring that challenges to a regime are outed in advance or quickly observed as they arise, and suppressed. This exposes US national security to risk.

In a world where citizen revolt tops the list of authoritarian fears, digital authoritarianism promises a set of solutions: Internet Protocol (IP) address lists used to block foreign online content; traffic header inspection to monitor online activity; legal control of Internet Service Providers (ISPs) whenever the government wants to shut down Internet services; and more. Sometimes, this is quite explicit. The Russian government, for instance, strongly promotes information control in domestic cyberspace for this reason.[4]

Other times, the suggestion is more subtle, for example when countries cite fake news and online disinformation as reasons to censor content deemed politically undesirable by those in power.[5]

In either case, authoritarian fears of protest and revolt have long driven such regimes to monitor their citizens. The difference today, however, is that digital technologies, like Internet packet inspection software and artificial intelligence (AI) facial recognition, are increasingly making it cheaper for dictators to do so. These technologies also make surveillance more scalable. They also reduce some of the risks caused by relying on massive networks of human spies and informants.[6] Steven Feldstein points out, for example, that the principal-agent problem, where, by empowering agents to spy and suppress, regimes empower them to act against the government, is a vulnerability that can be reduced by substituting automated surveillance technologies for human beings.[7] In turn, these technologies can heighten the speed, scale, and accuracy of authoritarian surveillance.

All of this matters for US national security because promoting democracy and contesting authoritarianism is in the US national interest—and digital authoritarianism helps authoritarian regimes consolidate power. Despite the sometimes resilient nature of online social movements, quashing political organization can be easier than ever before if aided by comprehensive digital surveillance and control technologies.[8] Governments can black out communications, such as Internet servers or mobile cell towers, during revolt. They can censor troubling posts before they bubble into something bigger. They can also censor foreign-originated information that could challenge regime narratives. Most importantly, they can continuously monitor their population, including during relatively stable times, to anticipate movements that could undermine government power. In the wake of a series of revolts in the Middle East that were informed, influenced, and/or aided in part by social media and the melding of online and offline mobilization, digital authoritarians, and those striving for such ends, are using digital technologies, often dual-use, to safeguard against such threats.[9] As the Russian General Valery Gerasimov offered in 2013, "The information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy," making it "necessary to perfect activities in the information space, including the defense of our own objects [objectives]."[10]

Many of these governments like China, Russia, and Iran, are unaligned with the US on security issues. In the cyber domain, they might engage in everything from pervasive trade secret theft to cyber attacks on foreign countries' electrical grids. In more traditional ways, they also pose national security risks through such vectors as nuclear weapons, military buildup, territorial aggression against US allies and partners, and disrupting the international order.[11] While US bilateral relationships are complex, often interconnected, and never zero-sum, elements of those relationships already pose national security risks.

Likewise, other countries pursuing digital authoritarian practices may be hostile to US interests (and democratic interests more broadly) or be aligned with other powers that threaten

national security. Power consolidation by these regimes poses national security risks in various dimensions. In some cases, the export and diffusion of digital surveillance tools, as part of digital authoritarianism, also pose additional national security risks, the point of focus in the next section.

2. INCENTIVES FOR AUTHORITARIANS TO ENCOURAGE DIFFUSION OF SURVEILLANCE CAPABILITIES

Private firms worldwide legally or illegally have long been selling dual-use digital technologies that can be used to monitor web traffic and to censor information. That there is a global market for digital surveillance tools is old news.

Companies incorporated in democracies heavily export these dual-use technologies worldwide, including, in many documented cases, to despots.[12] Likewise, companies incorporated in autocracies sell dual-use technologies, including those that can be used for censorship and surveillance, to other authoritarian regimes.[13] Some studies suggest that democracies account for a far greater volume of surveillance technology exports, including to despots, despite attempts to restrict such exports.[14]

The pursuit of digital authoritarianism to bolster state power magnifies incentives for some countries to acquire dual-use surveillance tools, and for others to encourage their spread. China's state leadership, for instance, consistently has advocated a sovereign and controlled Internet governance model on the global stage, with practices like censorship and surveillance, as opposed to a global and open model supported by many liberal democracies.[15]

In tandem with this global diplomatic messaging, the Chinese government has reportedly conducted trainings on new media or information management with representatives from dozens of countries, many on record as pursuing restrictive online practices.[16] This has coincided with countries targeted by the Belt and Road Initiative passing cybersecurity laws that sometimes mirror laws already enacted in China, such as Vietnam's recent establishment of data localization requirements.[17] Causality remains unclear in this situation, and empirical questions remain to be answered about the underlying drivers of digital authoritarianism in different countries. Nonetheless, these patterns and events, coupled with exports of surveillance technologies from China, raise questions about Beijing's intentions to spread digital authoritarianism globally, including through a greater focus on, and/or endorsement of, the sale of digital surveillance and control capabilities.

This could amplify the aforementioned national security risks, should authoritarian countries acquire the tools and/or knowledge needed to bolster their power through digital surveillance. National security analysts have already flagged these potential risks across Africa. Many countries China has engaged with through its Belt and Road investments have acquired Chinese surveillance technology, potentially usable for oppressive purposes. For instance, Chinese

company exports of surveillance technology to the Ethiopian government have occurred alongside Chinese government investments.[18] Given China's history of spying on and suppressing political dissidents, this is hardly a benign fact, and Ethiopia is but one of several examples. Should China's leadership be intent on spreading digital authoritarianism worldwide, to include diffusion of surveillance tools, this likely could include countries aligned with China's national security and/or economic interests.

Like China, Russia has long advocated for cyber sovereignty on the international stage,[19] with President Vladimir Putin repeatedly emphasizing the importance of information control within a country's sovereign borders.[20] As noted above, Russian companies export surveillance and hacking technologies, especially to post-Soviet states.[21] Andrei Soldatov and Irina Borogan actually suggest that Russian surveillance technology exports to some of these countries are a better fit than Western-made surveillance applications, because Russian laws and procedures governing traffic interception are more compatible for these countries, and the technologies are tailored accordingly.[22] In either case, these surveillance technology exports need further study, and they clearly serve as tools of political influence in Russia's near-abroad.

As with China, the extent of the Russian government's direct involvement in and support of such exports needs further study, because the Kremlin's direct hand in these exports, while visible, is hardly transparent. The desire to spread digital authoritarianism may well incentivize the Kremlin to better spread its surveillance technologies, or to at least look the other way when they occur, and thereby consolidate power in the hands of Russian-aligned countries at the expense of US government interests. This also could threaten vulnerable democracies worldwide, and facilitate the so-called fracturing of the global Internet, as countries build out technical and legal regimes that filter the global and open Internet touching and running through their borders.[23]

Again, the threat here is not only from governments in China and Russia. Companies incorporated in democracies also sell a high volume of dual-use surveillance technologies to despots, and this is something we are better able to monitor and correct. It is also important to reemphasize the existing incentives for countries to encourage or allow the spread of these capabilities to other countries (including the technologies and how to optimize them). But growing desires to spread digital authoritarianism globally not only undermine human rights and developing democracies; this also exposes US national security to increased risk.

3. INSULATION FROM FOREIGN CYBER ATTACKS AND LOWERED DISINCENTIVES TO DISRUPT GLOBAL INTERNET

Growing digital authoritarianism is manifested in more countries cracking down on Internet freedom within their borders, as they develop or acquire technical mechanisms to spy on and censor online information. This aspect of broader state control of the Internet has been

referred to as "cyber sovereignty."[24] Some countries have begun to alter cyberspace itself—for instance, how traffic flows from A to B, or what kinds of traffic can flow in the first place. This evolving global Internet landscape obviously impacts national cybersecurity and military cyber operations, by, among other ways, insulating certain actors from vulnerabilities, shifting the landscape of Internet connectivity in foreign countries, and potentially degrading foreign actors' effective disincentives to hack others.

Russia recently pressed to establish a domestic Russian Internet—an objective Kremlin officials have discussed for years. This was spurred in part, according to supporters, by an "aggressive" 2018 US cybersecurity strategy, referring to the White House's new cyber strategy published in the fall of 2018.[25]

There are undoubtedly other motivations for a domestic internet; in particular, the Kremlin leadership has sought more than ever, over the past few years, to control online traffic flows into, out of, and within Russia's borders.[26] Absent the scaled and sophisticated censorship infrastructure of its Chinese counterparts, isolating the Internet may be an easier Internet control solution for Russian leadership. Together, though, these motivations for Internet control and defense against foreign cyber threats have fueled the Kremlin's pursuit of a domestic internet that can be cut off from the rest of the world and still function under state management.

Russia's plans for isolating its Internet include granting the country's Internet regulator enhanced control over key "traffic exchange points," and allowing that same regulator to centralize the management of the Russian Internet in cases where its "integrity, stability, and security" appear at risk. These plans also include building a national Domain Name System (DNS) for Russia, thereby centralizing management and control of Internet traffic routing into and out of Russian territory.[27] Clearly, this is no easy lift; political and technical challenges remain for implementation.[28] In part, this may explain why a purportedly planned "disconnection test" of the Russian Internet[29] has yet to go forward. Yet, should this plan for a domestic Internet ultimately even partly succeed (e.g., the state consolidates more control over traffic routing, or Internet companies in Russia fall even more directly under Kremlin control), it is possible that Russia could better insulate itself from foreign cyber activity, both malicious and benign.

Enhanced control over Internet infrastructure and traffic flow and domination of the Internet within a country to reduce vulnerability to foreign cyber attacks has a potentially troublesome side effect, and that could be to reduce the Russian government's disincentives to attack or manipulate the more open Internet systems of others.

On the first point, vulnerability, US vulnerability to cybercrime, nation-state computer network operations, and other undesirable or malicious cyber behavior stems not only from issues like poor device security-by-design, but also from our relatively open Internet connectivity. The open connectedness of the US to the global Internet means myriad paths into US-based devices, networks, and infrastructure exist, and also, that operations targeting internet routing protocols can have a greater adverse impact on the US. For instance, manipulations of the Border

Gateway Protocol, which routes global Internet traffic, already have caused notable volumes of US Internet traffic to be unexpectedly routed through other countries, including China.[30] This could have serious economic and national security implications depending on the attack scenario.

Apart from other reduced vulnerabilities, if a country like Russia is far less dependent upon global Internet routing protocols, because it has built out its own DNS—that country may also be less susceptible to attacks that target protocols on the global side. As cyberspace within certain borders changes, other countries may have to alter exactly how cyber operations relating to that country must be conducted. This obviously impacts US military and Intelligence Community cyberspace operations, and that of our allies and partners, in ways often more drastic than mere routine additions, disconnections, updates, and relocations of devices and systems on the target country Internet. (Note: This need not be a negatively impactful change; centralizing management of the DNS within Russia, for instance, could actually make that country more vulnerable to Internet hijackings should a foreign country or criminal entity desire it.[31])

On the second point, disruption of incentives, the Kremlin already views its domestic internet plans in the context of decreased reliance on the global Internet, which President Putin casts as a CIA project,[32] and which the Kremlin continually tries to prove untrustworthy to justify its ever tightening Internet control.[33] The Russian government, which professes to be a victim of US cyber aggression, itself is a major destabilizing actor in cyberspace: conducting extensive online influence operations, from Ukraine to Turkey to Germany to the US;[34] launching large-scale global attacks like the NotPetya ransomware that caused billions of dollars in damage to the global economy;[35] and hacking and turning off the power grid in Ukraine.[36] Clearly, strong incentives drive the Kremlin to order, support, and allow cyber and information operations that use the Internet for destabilizing purposes abroad.

If Russia becomes increasingly less reliant on global networks, and hence perceives itself less vulnerable to foreign cyber-attacks, whether or not that perception is reality, this could reduce the disincentives for the Russian government to conduct even more destabilizing cyber operations.[37] Manipulating the Internet protocols of others, for instance, may present a more compelling option to sow chaos abroad and to undermine trust in the global Internet if the Kremlin feels insulated from retaliation in kind. Hence, growing digital authoritarianism on the Internet in the form of web isolation, therefore stands to impact global cybersecurity and US national security not only in how it changes the nature of the domain, but also the perceived consequences and incentives at play for state actors.

CONCLUSION

If and as other countries move in a direction similar to Russia—such as Iran, which continues to pursue its goal of a completely domestic Iranian Internet[38]—digital authoritarianism increasingly will implicate the layout and behavior of cyberspace itself. This also may diminish

disincentives against malicious cyber behavior, and change how cyber operations are conducted against such actors. Despite a concerted US focus on norm-development in cyberspace, the tracking and management of these changes to the layout and behavior of cyberspace (for example, which cables are cut, and how are protocols designed and redesigned?) are equally, if not more, important to encouraging reduced offensive cyber behavior by bad faith actors.

The risks that digital authoritarianism will bolster the power of authoritarian states, encourage the diffusion of dual-use surveillance and computer penetration technologies, insulate some regimes from foreign cyber-attacks, and degrade disincentives for certain regimes to engage in offensive cyber operations all impact US national security. Digital authoritarianism also obviously has serious implications for human rights and global democracy. This, normatively speaking, is more than reason enough for top leadership in the US to devote serious attention and resources to the issue. But the US military, including the entire national security establishment, increasingly will also find itself impacted by the worldwide spread of digital authoritarianism around the world, and should be proactively focused on this threat now.

NOTES

1. The author would like to thank Robert Morgus and Deb Crawford for their comments on an earlier draft of this article.
2. I first offered this general definition in Justin Sherman, "India's Digital Path: Leaning Democratic or Authoritarian?" *Just Security*, February 4, 2019, https://www.justsecurity.org/62464/indias-digital-path-leaning-democratic-authoritarian/. Other prominent uses of this phrase can be found in Freedom House, "Freedom on the Net 2018," October 2018, https://freedomhouse.org/report/freedom-net/freedom-net-2018; and Nicholas Wright, "How Artificial Intelligence Will Reshape the Global Order," *Foreign Affairs*, July 10, 2018, https://www.foreignaffairs.com/articles/world/2018-07-10/how-artificial-intelligence-will-reshape-global-order.
3. For instance, there is a consideration that the "authoritarianism" element of "digital authoritarianism" is an imprecise way to characterize digitally undemocratic or digitally illiberal practices that may be spread across, and occur differently in, various regime types that are not necessarily, by a very academic definition, "authoritarian."
4. Justin Sherman, "Russia's Tightening Control of Cyberspace Within Its Borders," *Just Security*, December 24, 2018, https://www.justsecurity.org/62023/russias-tightening-control-cyberspace-borders/.
5. Freedom House, "Freedom on the Net 2018," October 2018, https://freedomhouse.org/report/freedom-net/freedom-net-2018.
6. Justin Sherman, "Digital authoritarianism and the threat to global democracy," *Bulletin of the Atomic Scientists,* July 25, 2019, https://thebulletin.org/2019/07/digital-authoritarianism-and-the-threat-to-global-democracy/.
7. Steven Feldstein, "The Road to Digital Unfreedom: How Artificial Intelligence is Reshaping Repression," *Journal of Democracy*, Vol. 30, Issue 1 (Jan., 2019), 40-52.
8. Zeynep Tufekci, *Twitter and Teargas: The Power and Fragility of Networked Protest,* Yale University Press: New Haven, CT (2017).
9. Ibid.
10. Valery Gerasimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Military Review*, January-February 2016, https://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf 27. Translated from Russian into English by Robert Coalson on June 21, 2014, from *Military-Industrial Kurier*, February 27, 2013.
11. Several of these points on more "traditional" threat vectors are pulled from Amy Zegart, "The President's National Security In-Box," Stanford University, October 11, 2016, https://medium.com/@election2016stanford/the-presidents-national-security-inbox-c1220944acf5.
12. Robert Morgus and Justin Sherman, "How U.S. surveillance technology is propping up authoritarian regimes," *The Washington Post*, January 17, 2019, https://www.washingtonpost.com/outlook/2019/01/17/how-us-surveillance-technology-is-propping-up-authoritarian-regimes/.
13. Among many other news stories and analyses about companies incorporated in the likes of China and Russia exporting dual-use surveillance and digital control technologies, see Daniel Benaim and Hollie Russon Gilman, "China's Aggressive Surveillance Technology Will Spread Beyond Its Borders," *Slate*, August 9, 2018, https://slate.com/technology/2018/08/chinas-export-of-cutting-edge-surveillance-and-facial-recognition-technology-will-empower-authoritarians-worldwide.html; and Samuel Woodhams, "How China Exports Repression to Africa," *The Diplomat*, February 23, 2019, https://thediplomat.com/2019/02/how-china-exports-repression-to-africa/.
14. Privacy International, "The Global Surveillance Industry," Privacy International, July 2016, https://www.privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf, cited in Steven Feldstein, "Can a U.N. Report Help Rein in Expansive and Abusive Digital Surveillance?" *World Politics Review*, July 9, 2019, https://www.worldpoliticsreview.com/articles/28016/can-a-u-n-report-help-rein-in-expansive-and-abusive-digital-surveillance.
15. Robert Morgus, Jocelyn Woolbright, and Justin Sherman, "The Digital Deciders: How a group of often overlooked countries could hold the keys to the future of the global internet," New America, October 23, 2018, https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/.
16. Freedom House, "Freedom on the Net 2018," Freedom House, October 2018, https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf, 8.
17. Ibid.

NOTES

18. Human Rights Watch, "Ethiopia: Telecom Surveillance Chills Rights," March 25, 2014, https://www.hrw.org/news/2014/03/25/ethiopia-telecom-surveillance-chills-rights; Xinhua, "Upcoming Belt and Road forum to inject new momentum to Ethiopia infrastructure dev't drive," *Xinhua,* April 19, 2019, http://www.xinhuanet.com/english/2019-04/19/c_137988653.htm; and Amy Hawkins, "Beijing's Big Brother Needs African Faces," *Foreign Policy,* July 24, 2018, https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/.
19. Robert Morgus, Jocelyn Woolbright, and Justin Sherman, "The Digital Deciders: How a group of often overlooked countries could hold the keys to the future of the global internet," New America, October 23, 2018, https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/.
20. This extends far beyond just the Internet, although that is the focus here. For instance, see Jill Dougherty, "How the Media Became One of Putin's Most Powerful Weapons," *The Atlantic,* April 21, 2015, https://www.theatlantic.com/international/archive/2015/04/how-the-media-became-putins-most-powerful-weapon/391062/. Also see later footnotes for sources on "information security" in Russia.
21. Peter Bourgelais, "Commonwealth of Surveillance States: On the Export and Resale of Russian Surveillance Technology to Post-Soviet Central Asia," Access Now, 2013, https://www.accessnow.org/cms/assets/uploads/archive/docs/Commonwealth_of_Surveillance_States_ENG_1.pdf.
22. Andrei Soldatov and Irina Borogan, "In Ex-Soviet States, Russian Spy Tech Still Watches You," *Wired,* December 21, 2012, https://www.wired.com/2012/12/russias-hand/.
23. Justin Sherman and Robert Morgus, "Authoritarians Are Exporting Surveillance Tech, and With It Their Vision for the Internet," Council on Foreign Relations, December 5, 2018, https://www.cfr.org/blog/authoritarians-are-exporting-surveillance-tech-and-it-their-vision-internet.
24. For instance, see a discussion of cyber sovereignty by a member of the Cyberspace Administration of China: Lu Wei, "Cyber Sovereignty Must Rule Global Internet," *The Huffington Post,* February 14, 2015, https://www.huffpost.com/entry/china-cyber-sovereignty_b_6324060.
25. Robert Morgus and Justin Sherman, "Analysis: Russia's Plans for a National Internet," New America, February 19, 2019, https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/russias-plans-for-a-national-internet/.
26. Justin Sherman, "Russia's Tightening Control of Cyberspace Within Its Borders," *Just Security,* December 24, 2018, https://www.justsecurity.org/62023/russias-tightening-control-cyberspace-borders/.
27. Robert Morgus and Justin Sherman, "Analysis: Russia's Plans for a National Internet," New America, February 19, 2019, https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/russias-plans-for-a-national-internet/.
28. Among other analyses of the challenges at hand for Russia, see Charlotte Jee, "Russia wants to cut itself off from the global internet. Here's what that really means," *MIT Technology Review,* March 21, 2019, https://www.technologyreview.com/s/613138/russia-wants-to-cut-itself-off-from-the-global-internet-heres-what-that-really-means/; and Robert Morgus and Justin Sherman, "Is the Russian Internet a Lost Cause?" *Slate,* March 28, 2019, https://slate.com/technology/2019/03/russian-internet-runet-fragmentation-isolation.html.
29. Catalin Cimpanu, "Russia to disconnect from the internet as part of a planned test," *ZDNet,* February 11, 2019, https://www.zdnet.com/article/russia-to-disconnect-from-the-internet-as-part-of-a-planned-test/.
30. Chris C. Demchak and Yuval Shavitt, "China's Maxim – Leave No Access Point Unexploited: The Hidden History of China Telecom's BGP Hijacking," *Military Cyber Affairs,* Vol. 3 (Issue 1), 2018, 1-9, https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1050&context=mca.
31. This is not to advocate for the position of manipulating others' Internet protocols, but merely to clarify that the drastic changes to a country's Internet that may occur with Internet isolation policies could be harmful, beneficial, or benign to a foreign military's cyber operations against said country..
32. Ewan MacAskill, "Putin calls internet a 'CIA project' renewing fears of web breakup," *The Guardian,* April 24, 2014, https://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia.

NOTES

33. Kremlin efforts on the international stage over the past several years emphasize Internet insecurity and, as a direct consequence, the need for the state to tightly control the Internet as opposed to solutions to cyber insecurity that have been proposed in more democratic countries. For discussion of this fact and motivations at play, see, among others: Alex Grigsby, "Will China and Russia's Updated Code of Conduct Get More Traction in a Post-Snowden Era?" Council on Foreign Relations, January 28, 2015, https://www.cfr.org/blog/will-china-and-russias-updated-code-conduct-get-more-traction-post-snowden-era; Sarah McKune, "An Analysis of the Information Code of Conduct for Information Security," The Citizen Lab, September 28, 2015, https://citizenlab.ca/2015/09/international-code-of-conduct/; David Ignatius, "Russia is pushing to control cyberspace. We should all be worried," *The Washington Post*, October 24, 2017, https://www.washingtonpost.com/opinions/global-opinions/russia-is-pushing-to-control-cyberspace-we-should-all-be-worried/2017/10/24/7014bcc6-b8f1-11e7-be94-fabb0f1e9ffb_story.html; and Geoff Van Epps, "Common Ground: U.S. and NATO Engagement with Russia in the Cyber Domain," 2013, https://www.jstor.org/stable/26326340, 27.
34. Alina Polyakova, "Want to know what's next in Russian election interference? Pay attention to Ukraine's elections," Brookings Institution, March 28, 2019, https://www.brookings.edu/blog/order-from-chaos/2019/03/28/want-to-know-whats-next-in-russian-election-interference-pay-attention-to-ukraines-elections/; Katherine Costello, "Russia's Use of Media and Information Operations in Turkey," RAND Corporation, 2018, https://www.rand.org/pubs/perspectives/PE278.html; Michael Carpenter, "Undermining Democracy: Kremlin Tools of Malign Political Influence," Testimony before the U.S. House of Representatives Subcommittee on Europe, Eurasia, Energy, and the Environment, May 21, 2019, https://docs.house.gov/meetings/FA/FA14/20190521/109537/HHRG-116-FA14-Wstate-CarpenterM-20190521.pdf; and Erik Brattberg and Tim Maurer, "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks," Carnegie Endowment for International Peace, May 23, 2018, https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435.
35. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyber Attack in History," *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
36. Donghui Park, Julia Summers, and Michael Walstrom, "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks," University of Washington, October 11, 2017, https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.
37. This discussion of insulation from foreign cyber attacks is a build-out of a point briefly made in: 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/.
38. Ibid., and BBC, "Iran rolls out domestic internet," *BBC,* August 29, 2016, https://www.bbc.com/news/technology-37212456.

The Dr. House Approach to Information Warfare

Stefan Soesanto

Defending against information warfare across the vastness of the social media space is difficult, if not impossible, or so the story goes. Many are trying, many are failing, and we have all heard of the many solutions that will turn the tide someday, somewhere, somehow: increased media literacy, expanded factchecking, banning bots, deleting accounts, redirecting users, curtailing free speech, boosting counter-messaging, etc. But what if there were one solution, better than all others, that no democratic nation dares to touch ... yet?

The approach this paper outlines draws deep inspiration from the TV character Dr. Gregory House, played by Hugh Laurie, in the widely acclaimed US hospital drama *House*. Over the course of eight seasons, the "fascinatingly unsympathetic,"[1] "self-pitying, deeply sarcastic and sometimes smug"[2] medical genius of Dr. House captured audiences across the globe with his "straight, no-chaser approach to patient care."[3] House's thinking is perfectly summarized in the show's pilot, when his colleague Dr. Foreman asks: "Isn't treating patients why we became doctors?" to which House retorts, "No, treating illnesses is why we became doctors. Treating patients is what makes most doctors miserable."[4]

This article takes the Dr. House approach, with all its dark, provocative, and unconventional wisdom, and applies it to information warfare. Thus, in the same vein as House's cases hit eerily close to home and showcased the fallibility of the medical system, this article calls out the failures and misconceptions of current defensive strategies in the information warfare space to craft a better path forward. First, let us recap the problem we are trying to solve.

© 2021 Stefan Soesanto

Stefan Soesanto is a Senior Researcher on the Cyber Defense Team at the Center for Security Studies (CSS) at ETH Zurich. Before joining CSS, he was the Cybersecurity & Defense Fellow at the European Council on Foreign Relations (ECFR) and a non-resident James A. Kelly Fellow at Pacific Forum CSIS. At ECFR, he designed and held cyber wargame exercises in cooperation with Microsoft, and organized a closed Cybersecurity and Defense conference in Odense together with the Center for War Studies at the University of Southern Denmark and the Office of the Danish Tech Ambassador. He also served as a Research Assistant at RAND's Brussels office, co-authoring reports for the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE), the European Network Information Security Agency (ENISA), and the Dutch Ministry of Security and Justice.

Information warfare operations encompass a wide range of strategies, tactics, tools, goals, and motivations. In the broadest terms, info ops can be divided into two categories: Morale operations, which the U.S. Office of Strategic Services (OSS) defined in 1943 as, "all measures of subversion–other than physical–used to create confusion and division, and to undermine the moral and the political unity of the enemy through any means,"[5] and political warfare operations, which, according to Angelo Codevilla, is the "marshaling of human support, or opposition, in order to achieve victory in war or in unbloody conflicts as serious as war."[6] In other words, while the former seeks to sow chaos and division, the latter aims to generate trust and unity amid likeminded groups. Naturally, there are numerous spillover effects between the two categories, particularly on social media platforms specifically designed to facilitate relationships and build trust through continuous content engagement.

At its most elemental level, every information warfare operation is an input-output communication cycle. Operators post a message, image, or video, which intermediaries carry, through algorithms, relationships, hashtags, etc., to a target audience to elicit a response. Given the operator's visibility as to how his product moves (retweets, likes, reverse image searches, etc.), the operation can leverage real-time social network analysis and initiate a feedback loop to tailor his messaging and fine-tune the trust-building process to gain credibility, authority, and importance within the target network. Operations will sometimes run on top of pre-existing beliefs and emotions to radicalize or strengthen opposition within a target group. Or they will create new emotions and new beliefs that run counter to existing ones. Static defenders cannot react timely or compete in this fast-paced dynamic environment.

But many elemental questions surrounding information warfare remain unresolved. Veteran information

security researcher The Grugq summarized it aptly in three sentences: "What [are] the adversary's most effective strategies, tactics, and tools? Where should [the defender] invest resources to mitigate [adversarial] strengths? [And] where should [the defender] invest resources to address [his own] weaknesses?"[7] From the defender perspective, it is extremely difficult to find credible metrics that reliably ascertain the effectiveness or impact of an adversarial information warfare operation. Daily, weekly, or monthly polling of the same target group may be an acceptable starting point to map changes in attitude and identify potential causal linkages. But doing so at scale outside of an election cycle would be expensive, tedious, and most likely result in diminishing returns over time as answers become repetitive and habitual. Similarly, identifying operations in their preparatory stages, such as a meme being tested "in-house," provides little to no value if the target group cannot take reasonable defensive actions, or is overwhelmed by the sheer volume of incoming threat intelligence.

Absent reliable information warfare metrics, defenders have veered in their fight against what RAND calls "truth decay" toward user trust generating solutions and an increase in platform responsibilities.[8] On the trust side, the aim is to change how information is consumed. Solutions range from increasing media literacy,[9] spreading user awareness on propaganda,[10] to providing easy access to open-source tools that fact-check items or rate entire news outlets on their trustworthiness.[11] On the platform end, the goal is to change how information moves. YouTube, for instance, demonetized and deleted accounts that feed into certain political narratives,[12] WhatsApp limited the number of users to which a single message can be forwarded,[13] and Facebook increased the visibility of political ads by disclosing their sources of funding.[14]

The limits of the current information-centered approach become apparent in a simple thought experiment. Let us assume that platforms are continuously "politically-cleansed" and the average user is "resilient." Instead of seeing beliefs and opinions move toward the political center, the overall political discourse outside the platform environment will most likely veer into the opposite direction and become more radical, divisive, and siloed. If we take the US, for example, the reasons for this negative trend are straightforward. First, audience mapping is showing repeatedly that the majority of "reliable" US news outlets are not seen to be situated in the political center. [15] Second, increased media literacy and higher education do not translate into apolitical and non-radical views. In fact, proponents of media literacy have long championed the notion that they actually encourage political engagement,[16] and a 2018 World Bank study based on leaked Islamic State records found that "higher education seems to be associated with high intrinsic motivation to join the terror group."[17] Third, political content moderation always creates winners and losers, particularly if it is leveraged against truthful content that has been reframed (i.e., is the glass half-full or half-empty?), or when it is purposefully exploited to push a political agenda. This can range from suspended Twitter accounts of Chinese political dissidents ahead of the 30th anniversary of the Tiananmen massacre[18] to activists feeding the social media outrage machine in an effort to push a platform to act beyond its community

platform standards.[19] Lastly, while fake news and outright lies naturally struggle with limited shelf life and constrained reach, memes, rumors, and half-truths will never stop resonating with political beliefs, emotions, and prejudices held offline.

If the current defense posture does not push hard enough against the underlying information warfare dynamics, or worse, allows counter-productive results in the real world, can we think up a better way to fight back? Enter the Dr. House approach to information warfare.

Instead of focusing on information as the primary subject, Dr. House would take a social network analysis (SNA) point of view. This means, what matters most is not the message, image, or video posted, but the social network structure that moves the product. SNA has most notably been employed for counterterrorism and deradicalization purposes online, such as identifying ISIL users on Twitter and clustering related communities based on shared interactions.[20] SNA primarily uses open source information to display a network's structure as nodes (accounts) and edges (relationships) in line with graph theory to understand "how humans relate, communicate, and spread information."[21] While many different algorithms allow for visually ordering a network structure, two elements are considered standard measurement features: The number of edges of a node, which measures a node's network centrality, and how close a node is to other nodes measures a node's importance within the network.[22]

Once mapped, we can start thinking about network intervention strategies. Bargar, et al., identified four overarching techniques: (1) Identification techniques try to "engage actors in key positions in a network for training or messaging, with the expectation that their actions will impact the overall network." (2) Segmentation techniques are used to "intervene with an echo chamber as a collective set so all actors receive content simultaneously." (3) Induction techniques aim to "reframe a narrative by actively encouraging people to communicate with each other." And (4) alteration techniques seek to "modify a network structure by adding or deleting [edges] and/or nodes."[23]

All four techniques have one aspect in common: they seek to make the network healthier and less radical while respecting the user/patient rights. The Dr. House approach does the opposite. It wants to make the network sicker and sicker to the point of inducing cardiac arrest. In this context, user/patient rights do not matter, and finding a cure is merely the cherry on top. As Dr. House would put it, "Don't do what a patient wants. Do what a patient needs."

A second mental hurdle Dr. House throws out the window is the notion that to fight lies one must tell the truth. Facts against fiction, or a push for transparency and openness, are not the ingredients for a winning strategy in the information warfare space. Study after study has proven that lies travel faster than truths,[24] that fact-checking websites confront the same onslaught of disaffection and distrust that plagues "reliable" news outlets,[25] and that bursting echo chambers will most likely entrench partisan views rather than reduce biases and prejudices.[26] At its heart, the evidence points in only one direction: Facts do not create reality, and the information warfare space is an offense-dominant domain. Staunchly defending the truth

perimeter is simply not going to cut it, because in the world of Dr. House "everybody lies. The only variable is about what."[27]

The third mental hurdle that needs to vanish is the idea of asymmetry. Contrary to popular belief, the information warfare space is not an asymmetric space. Anyone can hit any target anywhere. The only limiting factors are language skills, cultural familiarity, and social media penetration within the target network. Strategically, everyone, apart from the platform owner, plays on the same level battlefield. The story is a bit different when we talk about operations and tactics. Those who know their offline audience best essentially dominate the network online, which is why Alex Stamos, former Chief Security Officer at Facebook, noted that "if you look globally at disinformation campaigns, the median victim of a professional disinformation campaign is a victim of a campaign being run by their own government."[28] In the English-speaking online world, the reality is reversed primarily because democratic governments seldom can gain political and legal approval to run disinformation campaigns against their own populations. Consequently, non-state actors reign supreme in this space. 4Chan's /pol/ is probably the best example of an English-speaking online community that is both resilient on the defensive end, and able to mobilize the most sophisticated offensive information warfare teams out there. Nudging /pol/ in a certain direction is extremely difficult, as members are inherently suspicious that the CIA, Mossad, the FBI, or any number of activist groups from across the political spectrum tries to run rumors, propaganda, and lies on its platform. The tin-foiled hat is certainly not undeserved as /pol/ has been the birthplace of many conspiracy theories and executed numerous successful information warfare campaigns over its eight years of existence.[29] However, given that the community worships Christchurch shooter Brandon Tarrant as a martyr and saint,[30] turned milk and the "ok" sign into white supremacy symbols,[31] and considers itself to be the home of "the most diverse group of people from all over the world to fight against diversity and globalism,"[32] it should hardly come as a surprise that /pol/ is widely seen as the dark underbelly of the Internet.[33] But no matter your political views on the content posted on /pol/, when it comes to information warfare, learning from /pol/ probably means learning from the best. As a teenage patient explains to a third-year medical student on House's team, "At the top of the game, you play by different rules."[34]

The fourth point Dr. House would seek to exploit is the notion that information warfare operations are difficult to execute. A sophisticated campaign takes a lot of preparation, which is why simply firing off a single tweet and hoping it will stick and go viral within a target community is not the professional way to go. As The Grugq explains, "You need to do a lot of research, you need to have a lot of material. You need to prepare all the stuff. Get your narratives ready and then build up your channels. Get your credibility and so on."[35] State and non-state actors essentially go through the same tedious planning process whether their campaigns are malicious or not. The only major difference is how and when they leverage certain instruments and tools within their individual campaigns. Russia's Internet Research Agency, for instance, relied heavily on agitprop,[36] sock puppets, useful idiots, and hacked documents to run its campaign

against the 2016 US Presidential Election.[37] /pol/ instead prefers to subvert existing beliefs and then let motivated individuals carry their products across the information space.[38] In late 2019, /pol/ ran a campaign that consisted of numerous A4 print-outs with the simple sentence "Islam is right about women" plastered around the sleepy town of Winchester, Massachusetts. Numerous local and regional news outlets naturally reported on the "incident," but clearly shied away from tackling the implied logic of the statement. Instead, Boston 25 News went on to report comically that "in Winchester, signs that read 'Islam was RIGHT about women' have residents scratching their heads to figure out exactly what the poster meant by those words. [...] 'I assume it's negative,' said Dorothy Kruger, a resident. 'That's not cool, that's not a cool thing to do."[39]

The only major exception to the planning rule encompasses spammers and scammers, who try to monetize disinformation campaigns based on sheer volume. That Nigerian prince trying to share his fortune with you if you just transfer a bit of money makes for a very effective campaign at scale, but is plain amateur hour when compared to a professionally run in-depth campaign. In House's words: "Welcome to the world. Everyone's different, everyone gets treated different. You try fighting that, you end up dying of TB."[40]

Turning now to the practical side of things, the Dr. House approach envisions a government agency, department, or state-affiliated actor to pro-actively defend society against information warfare campaigns in two ways.

The first option starts with mapping out networks and identifying possible adversarial campaigns. Importantly, the defender need not waste time and resources to conduct attribution or assigning political motivation as to why outrage is building around a specific issue or topic. The only relevant metric is whether the activity could potentially undermine national cohesion, break the civil political discourse, or threaten the overall functioning of society over time. If any of the three are met, the defender is mostly likely dealing with either a foreign state adversary or a motivated non-state actor. In both cases, the solution is to run an information warfare campaign on top of the adversarial one. Synchronize our nodes and edges with theirs, and gain centrality and importance within the existing network by being more extreme, but also qualitatively better, and quantitatively richer than anyone else in the network. By opening up the internal fight on network position, user mobilization, and content, we essentially take away the adversary's luxury of capturing the network unchallenged through mere radicalization tactics.

Once the combined network has reached a critical mass, the plan is for operators to burn down the barn with counter-messaging from the center out. The mathematical NP-hard problem that still needs to be solved to make this end game strategy successful is figuring out how many nodes and edges we would have to turn and burn to break a complex network into small, disconnected parts. Network science calls this the optimal network demolition problem,[41] which also closely relates to the yet unresolved optimal influence problem that tries to localize a specific set of structural nodes, that if activated, spreads the same information to every node

in the entire network.[42] According to Patron et al., research has so far concentrated on three types of network demolition attacks: random attacks, targeted attacks, and localized attacks.[43] In a random attack, "the attacker has no information about the network, its topology, or characteristics" and thus choses a fraction of nodes to be randomly destroyed. Social media companies and political activists are currently practicing this approach in pretty much all of their cleansing campaigns. In a targeted attack, "the attacker has some information about the topology and the nodes of the network," and thus "determines which nodes to attack and in which order." Meanwhile, in a localized attack, "the attack begins against one node" and then continues against its neighbors, and the neighbors of its neighbors, and so forth, until a certain fraction of the network is destroyed.[44] For our purposes, it is important to note that the Dr. House approach does not attack at random and does not need to concern itself with the order of node destruction. A 2015 Nature article by Kovacs and Barabasi is probably the better approach for network destruction, as it speculates that "it is not certain whether targeting and removing network hubs – defined as the nodes with the largest number of [edges] – can inflict maximum disruption on a network. It may be more effective to eliminate a combination of hubs and central, but less-well-connected, nodes."[45] These are the exact target positions Dr. House would seek to occupy.

What might complicate matters for the defender is that the same adversary will probably move on different platforms simultaneously forcing the defender to create cascading demolition effects that concurrently attack specific networks across multiple platforms. However, what does play in the defender's favor is that he is not only searching for the optimal damage calculus, but also injects fear, uncertainty, and doubt into the network by his very action. If members cannot trust and believe in the messaging coming out of the most central and important nodes in one network, then whom else can they trust and believe in on other platforms? Thus, rather than spreading the truth and trying to convince the network to take on a certain belief, Dr. House would want all nodes to put on their tin foil hats. Question everything, doubt everything, double-check everything – taking media literacy to the extreme. Notably, destroying networks and belief systems in such a way is not tantamount to erasing an individual's ability to make sense of reality nor his desire to create new trust relations over time. Just because you question, doubt, and double-check everything does not mean that you do not believe or trust in anything.

The second option employs an even more aggressive tactic. Instead of mapping and identifying adversarial networks, a defender will proactively search for exploitable political, social, and economic cracks in his society. Thus, rather than letting a contentious issue grow organically over time, the defender runs an information warfare campaign preemptively into those cracks to create networks artificially, thereby fighting from a position of centrality and importance and forcing the adversary to latch onto and synchronize with this artificial network. If executed well, the defender might even enjoy the luxury of total visibility on the specific

crack-issue, thus making mapping, nudging, and controlling the network much easier. On top of the network position advantage, this option also inserts doubts and uncertainty, forcing adversaries to continuously make cost-benefit calculations, and think twice before kicking off a tedious planning process and investing more scarce resources into radicalizing a network that might not be organically grown and is potentially controlled by a defender. The goal is to make an adversary so paranoid that he will doubt every action he takes in every network in which he operates.

One issue we have yet to tackle is where a government agency or non-state actor would get all the talent needed to run these vile and radical operations. The politically correct answer would be simply to hire people and train them in-house, but then again, how do you practically train someone to shitpost and express more radical thoughts than ISIL, the alt-right, and Antifa combined. The unconventional answer is to hire those who already wage information warfare for free in their spare time on platforms like 4Chan, Reddit, and Discord. Agencies would merely have to restrain and pull operators who lose themselves in the mission back into reality. There are even some ethical parallels that one could draw from how the cybersecurity community has embraced the hacker culture over the past decade. A similar transformation might be necessary in the information warfare space to fill the lack of talent, skills, and evil ingenuity.

In sum, today's thinking on information warfare self-curtails itself based on the misguided belief that "it's hard to fight fire with fire, especially when you can't use the same evil techniques, manipulations, and lies as the opposition employing propaganda against you."[46] The Dr. House approach is different. It is politically incorrect, violates numerous ethical standards, and is probably illegal in most states around the world. Maybe ... just maybe, though, it is time to give Dr. House a chance, because, as he argues in his own words, "I take risks, sometimes patients die. But not taking risks causes more patients to die, so I guess my biggest problem is I've been cursed with the ability to do the math."[47]

NOTES

1. Rob Owen, "TV Review: Hugh Laurie makes 'House' worth a visit," *Pittsburgh Post-Gazette,* November 14, 2004, https://web.archive.org/web/20081208154155/http://www.post-gazette.com/pg/04319/410715-237.stm.
2. Tom Shales, "House: Watching Is the Best Medicine," *The Washington Post*, November 16, 2004, http://www.washingtonpost.com/wp-dyn/articles/A53025-2004Nov15.html.
3. Paul Brownfield, "Obnoxious doctor in the 'House'," *The Los Angeles Times*, November 16, 2004, https://www.latimes.com/archives/la-xpm-2004-nov-16-et-house16-story.html.
4. House, Season 1, Episode 1: Pilot.
5. Office of Strategic Services, "Morale Operations Field Manual - Strategic Services," January 25, 1943, https://www.cia.gov/library/readingroom/docs/CIA-RDP89-01258R000100010002-4.pdf, 1.
6. Angelo M. Codevilla, "Political Warfare," in *Political Warfare and Psychological Operations–Rethinking the US Approach,* National Defense University Press–National Strategy Information Center, 1989, https://www.files.ethz.ch/isn/139664/1989-01_Political_Warfare_8-Chap.pdf, 77.
7. The Grugq, "After Action Reviews and Lessons Learned," *Medium.com,* December 3, 2018, https://medium.com/@thegrugq/after-action-reviews-and-lessons-learned-ec13218973c6.
8. Jennifer Kavanagh and Michael D. Rich, "Truth Decay – An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life," RAND Corporation, 2018, https://www.rand.org/pubs/research_reports/RR2314.html.
9. Marin Lessenski, "Common Sense Wanted – Resilience to 'post-Truth' and Its Predictors in the New Media Literacy Index 2018," Open Society Institute – Sofia, March 2018, http://osi.bg/downloads/File/2018/MediaLiteracyIndex2018_publishENG.pdf.
10. Jed Willard, "What Europe can teach America about Russian Disinformation," *The Atlantic*, June 9, 2018, https://www.theatlantic.com/international/archive/2018/06/what-europe-can-teach-america-about-russian-disinformation/562121/.
11. Issie Lapowsky, "Newsguard wants to fight fake news with humans, not algorithms," *Wired*, August 23, 2018, https://www.wired.com/story/newsguard-extension-fake-news-trust-score/.
12. Kelly Weill, "YouTube Crackdown on Extremism Also Deleted Videos Combating Extremism," The Daily Beast, June 6, 2019, https://www.thedailybeast.com/youtube-crackdown-on-extremism-also-deleted-videos-combating-extremism.
13. Jacob Kastrenakes, "WhatsApp Limits Message Forwarding in Fight against Misinformation," The Verge, January 21, 2019, https://www.theverge.com/2019/1/21/18191455/whatsapp-forwarding-limit-five-messages-misinformation-battle.
14. Rory Cellan-Jones, "Facebook Tool Makes UK Political Ads 'Transparent,'" *BBC News*, October 16, 2018, https://www.bbc.com/news/technology-45866129.
15. Nic Newman and Richard Fletcher, "Bias, Bullshit and Lies – Audience Perspectives on Low Trust in the Media," Reuters Institute for the Study of Journalism, 2017, https://agency.reuters.com/content/dam/openweb/documents/pdf/news-agency/report/nic-newman-and-richard-fletcher-bias-bullshit-and-lies-report.pdf, 19.
16. Paul Mihailidis and Benjamin Thevenin, "Media Literacy as a Core Competency for Engaged Citizenship in Participatory Democracy," *American Behavioral Scientist* 57, no. 11 (2013): 1611–22, https://pdfs.semanticscholar.org/8f26/be24b8669fe1a15832a5b9a4f96aa9db2790.pdf.
17. Mohammed Abdel Jelil et al., "Unemployment and Violent Extremism – Evidence from Daesh Foreign Recruits," World Bank Group, March 2018, http://documents.worldbank.org/curated/en/967561522155860057/pdf/WPS8381.pdf, 2.
18. Paul Mozur, "Twitter Takes Down Accounts of China Dissidents Ahead of Tiananmen Anniversary," *The New York Times*, June 1, 2019, https://www.nytimes.com/2019/06/01/business/twitter-china-tiananmen.html.
19. Jason Koebler and Mack Lamoureux, "YouTube Miserably Fails to Explain Why It Didn't Ban Steven Crowder," *Vice Motherboard*, June 5, 2019, https://www.vice.com/en_us/article/3k37yk/youtube-miserably-fails-to-explain-why-it-didnt-ban-steven-crowder-for-antagonizing-carlos-maza.
20. Elizabeth Bodine-Baron et al., "Examining ISIS Support and Opposition Networks on Twitter," RAND Corporation, 2016, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1328/RAND_RR1328.pdf.
21. Alicia Bargar et al., "Challenges and Opportunities to Counter Information Operations through Social Network Analysis and Theory," in *11th International Conference on Cyber Conflict: Silent Battle*, 231-48. NATO CCD COE Publications, n.d., https://ccdcoe.org/uploads/2019/06/CyCon_2019_BOOK.pdf, 232.

NOTES

22. Andrew Disney, "KeyLines FAQs: Social Network Analysis," *Cambridge Intelligence,* December 3, 2014, https://cambridge-intelligence.com/keylines-faqs-social-network-analysis/.
23. Alicia Bargar et al., "Challenges and Opportunities to Counter Information Operations through Social Network Analysis and Theory," In *11th International Conference on Cyber Conflict: Silent Battle,* 231– 48. NATO CCD COE Publications, n.d., https://ccdcoe.org/uploads/2019/06/CyCon_2019_BOOK.pdf, 245.
24. Soroush Vosoughi et al., "The Spread of True and False News Online." *Science* 359, no. 6380 (March 9, 2018): 1146–51, https://science.sciencemag.org/content/359/6380/1146.
25. Glenn Kessler, "Rapidly Expanding Fact-Checking Movement Faces Growing Pains," *The Washington Post,* June 25, 2018, https://www.washingtonpost.com/news/fact-checker/wp/2018/06/25/rapidly-expanding-fact-checking-movement-faces-growing-pains/?utm_term=.cadbd8fa4317.
26. Carolyn Y. Johnson, "Bursting People's Political Bubbles Could Make Them Even More Partisan," *The Washington Post,* September 7, 2018, https://www.washingtonpost.com/science/2018/09/07/bursting-peoples-political-bubbles-could-make-them-even-more-partisan/?utm_term=.cd44d9170bb4.
27. House, Season 1, Episode 21: Three Stories.
28. Victoria Kwan, "Facebook's Ex-Security Chief on Disinformation Campaigns: 'The Sexiest Explanation Is Usually Not True,'" *First Draft News,* July 9, 2019, https://firstdraftnews.org/alex-stamos-interview-disinformation-campaigns/.
29. Ben Schreckinger, "World War Meme." *Politico,* April 2017, https://www.politico.com/magazine/story/2017/03/memes-4chan-trump-supporters-trolls-internet-214856.
30. 4Chan /pol/, "Saint Tarrant," *Archive.4plebs.org,* March 19, 2019, https://archive.4plebs.org/pol/thread/206981854/ Tarant.
31. Joseph Bernstein, "The Trump Internet Keeps Making Fake Hate Symbols, And People Keep Falling For It," *Buzzfeed News,* April 30, 2017, https://www.buzzfeednews.com/article/josephbernstein/the-trump-internet-keeps-making-fake-hate-symbols-and.
32. /pol/ Memeball, "When you bring together the most diverse group of people from all over the world to fight against diversity and globalism," *KownYourMeme,* https://knowyourmeme.com/photos/1387762-picardia.
33. Gabriel Emile Hine et al., "Kek, Cucks, and God Emperor Trump: A Measurement Study of 4chan's Politically Incorrect Forum and Its Effects on the Web." *ArXiv,* 2017. https://arxiv.org/abs/1610.03452, 1.
34. House, Season 7, Episode 19: Last Temptation.
35. Zack Pokorny, "The Grugq Illuminates Influence Operations," *Recorded Future,* March 25, 2019, https://www.recordedfuture.com/podcast-episode-100/.
36. The Grugq, "Russian Propaganda Isn't Even That Good," *Medium.com,* November 8, 2018, https://medium.com/@thegrugq/russian-propaganda-isnt-even-good-c438f7d49902.
37. U.S. House of Representatives, "Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements," Permanent Select Committee on Intelligence, n.d., https://intelligence.house.gov/social-media-content/.
38. 4Chan /pol/, "Operation Rainbow," *Archive.4plebs.org,* April 24, 2017, https://archive.4plebs.org/pol/thread/122568047/.
39. Boston 25 News, "'Islam is right about women': Odd signs spark confusion in local town," Boston 25 News, September 18, 2019, https://www.boston25news.com/news/-islam-is-right-about-women-odd-signs-spark-confusion-in-local-town/987837653.
40. House, Season 2, Episode 4: TB or Not TB.
41. Istvan A. Kovacs and Albert-Laszlo Barabasi, "Destruction Perfected." *Nature,* August 6, 2015, 524 edition, https://www.nature.com/articles/524038a?proof=true&draft=journal.
42. Flaviano Morone and Hernan A. Makse, "Influence Maximization in Complex Networks through Optimal Percolation," *Nature,* August 6, 2015, 524 edition, https://www.nature.com/articles/nature14604.pdf, 65.
43. Amikam Patron et al., "Optimal Cost for Strengthening or Destroying a given Network," *Physical Review W* 95, no. 5 (May 2017). https://arxiv.org/pdf/1705.09930.pdf, 1.
44. Amikam Patron et al., "Optimal Cost for Strengthening or Destroying a given Network," *Physical Review W* 95, no. 5 (May 2017), https://arxiv.org/pdf/1705.09930.pdf, 1.

NOTES

45. Istvan A, Kovacs and Albert-Laszlo Barabasi, "Destruction Perfected." *Nature,* August 6, 2015, 524 edition, https://www.nature.com/articles/524038a.pdf?proof=true&draft=journal, 38.

46. Guy Bergstrom, "How to Defend Against Rumors, Lies, and Propaganda," *The Balance Small Business*, February 18, 2019, https://www.thebalancesmb.com/defending-against-rumors-lies-and-propaganda-2295244.

47. House, Season 1, Episode 11: Detox.

THE CYBER DEFENSE REVIEW

RESEARCH NOTE

Information Influence Operations: The Future of Information Dominance

Captain David Morin

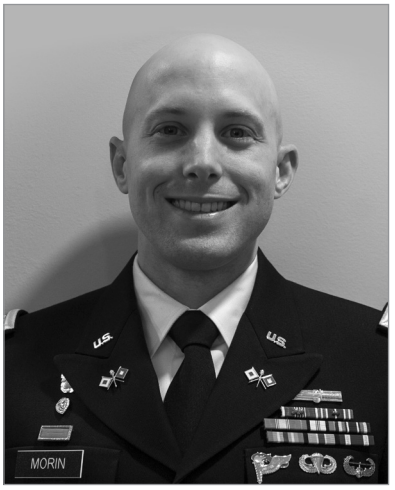
ABSTRACT

This paper proposes the development and inclusion of Information Influence Operations (IIOs) in Cyberspace Operations. IIOs encompass the offensive and defensive use of cyberspace to influence a targeted population. This capability will enable the evolution of strategic messaging in cyberspace and allow response to near peer efforts in information warfare.

INTRODUCTION

This paper proposes that Information Influence Operations (IIOs) be developed and utilized within U.S. Cyber Command's (USCYBERCOM) capability set. When correctly employed, IIOs will become a critical capability that is key to the future of cyberspace operations. IIOs must become the new "light touch", the guiding hand gently pushing public opinion, and ultimately shaping global perception and narratives in support of US strategic interests. LTG Stephen Fogarty stated: "the command [Army Cyber Command] must mimic enemy capabilities and better integrate and synchronize information operations, military deception, psychological operations, electronic warfare, all intelligence disciplines."[1] Today, most leaders consider cyber effects either an intelligence collection source or a means of causing real-world impact, such as turning off a power grid or causing significant disruption to an enemy's C2 network. Those views require revision to take full advantage of the value of cyberspace. The unrealized value of cyberspace, and what makes it so dangerous, is it allows direct access to the individual and to the public at large. This access, when used correctly, provides actors in cyberspace the ability to influence public opinion and shape the narrative of ongoing operations.

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



Captain David Morin is currently serving as the Company Commander of the 93d Signal Brigade Headquarters and Headquarters Company. He is from Washington, DC, and was commissioned as an officer in the Army in 2013 after earning bachelor's and master's degrees in engineering from Washington University in Saint Louis. His previous positions and assignments include Brigade Senior Network Officer (93d Signal Brigade), Battalion S6 (704th Brigade Support Battalion, 2/4ID), and Base Defense Engineer (3-62 Cavalry Squadron, 2/4ID). CPT Morin is a graduate of the Armor Basic Officer Course, the Signal Captains Career Course (SCCC), the Joint Command Control Communications and Computers Course (JC4PC), and the Joint Command Control Communications and Computers Intelligence Cyber Staff Operations Course (JC4ICSOC). He is the first signal officer to earn the Expert Soldier Badge and has also earned the Pathfinder, Airborne, and Air Assault Army qualifications and seven IT Certifications.

BACKGROUND

Unsurprisingly, senior leaders' perceptions of cyber capabilities have been shaped by popular culture and the more infamous cyber incidents and attacks. There is a plethora of apocalyptic examples of hypothetical cyber-attacks as portrayed in popular movies: *War Games* (1983), *Hackers* (1995) *Live Free or Die Hard* (2007), and *Skyfall* (2012). In all these movies, the world is nearly brought to a halt due to a single or series of cyber-attacks against military equipment, the internet or other critical infrastructure. All these fictional depictions are reinforced by reporting on some of the most well-known real-world cyberattacks such as Stuxnet, NotPetya, and the Russian actions surrounding the 2016 U.S. Presidential elections.[2] The first two of these attacks resulted in overt denial of resources and damage to equipment. Stuxnet could target almost any type of infrastructure, but was specifically designed to act against Iranian centrifuges.[3] NotPetya, a piece of ransomware with unconfirmed attribution to Russian cyber forces, was based on a leaked NSA toolkit that was substantially less targeted and as a result inflicted over $10 billion in damage worldwide as systems were rendered useless.[4] The last of these attacks, the election interference, will be the longest-lasting in its effects. "The IRA [Internet Research Agency] later used social media accounts and interest groups to sow discord in the US political system through what it termed "information warfare." The campaign evolved from a generalized program designed in 2014 and 2015 to undermine the US electoral system"[5] This offensive should be taken as a proof-of-concept in that it shows the real power of cyberspace operations, the capability to manipulate perception on a massive scale. IIOs, if developed and utilized properly, will become an incredibly powerful tool for achieving US goals in the information battlespace or even the geopolitical realm.

INFLUENCERS

As communications technology and the Internet have proliferated, capabilities previously limited to major companies and government are now accessible to anyone with an Internet connection. The traditional consumers of news can now play a major part in producing it. Bob Franklin and Lily Canter assert that "Advances in technology have profoundly impacted war reporting, affording audiences new ways in which to visualize conflict. Satellites, smartphones, laptops, and mobile broadband have enabled war reporters to communicate immediately and bring conflict live to air. Nevertheless, as new technologies open up innovative ways for journalists to convey the horrors of warfare, they similarly create opportunities for propaganda, censorship, and control."[6] The communications capabilities referenced have contributed to the creation of a power vacuum in the information realm of cyberspace. This vacuum is being filled not by traditional media and governments but by small groups of content creators and "influencers" whom have rapidly capitalized on the massive reach provided by new technologies. These "influencers" are capable of wielding influence over millions and have used this influence for a multitude of purposes from philanthropy and advertising to political ends. The future of cyber operations is the use of IIOs in cyberspace to wield influence.

The beginning of this evolution for institutional influence of information can be seen most easily through the creation and employment of state-sponsored media. While some governments have chosen to use this influence capability to maintain a well-informed public, others have begun to use the capability to explicitly influence opinion. The British Broadcasting Corporation's (BBC) mission statement is "to act in the public interest, serving all audiences through the provision of impartial, high-quality and distinctive output and services which inform, educate and entertain."[7] The BBC's mission is a prime example of the first use, simply to create a more engaged and informed populace. Its mission explicitly states that it endeavors to deliver an impartial rendering of the facts. According to recent public surveys, many believe that the BBC is effectively fulfilling this mission.[8]

In comparison, Russia Today (RT) explains its mission as: "RT creates news with an edge for viewers who want to Question More. RT covers stories overlooked by the mainstream media, provides alternative perspectives on current affairs, and acquaints international audiences with a Russian viewpoint on major global events."[9] RT admits that it is not necessarily an impartial reporter of the facts. This is important because 80% of what RT reports is factual news reporting. However, the other 20% is the part that is used more overtly to shift its audience's opinions.[10] If "unbiased" media sources continue to perform their stated mission of informing the public, they can occasionally be covertly leveraged to sway opinion or counter other sources of influence. They sway their audiences by simply continuing to report the same news and facts, but in slightly different ways. It is important to understand how organizations orient their audiences and for what purpose: to inform the public, sell more content, sow discord in a population, or spur political change.

INFLUENCE CAMPAIGNS

The future of cyber operations is to determine how to influence the public and work to regain and retain the ability to protect the narrative of our long-term strategy and vision for the world by shaping the perception of that narrative. We must develop the ability not only to dam a river, but to throw a pebble into a river and, imperceptibly but substantially, shift its flow. This subtle action must be the new paradigm for IIOs. Small imperceptible adjustments to the availability of information will enable the modification of the narrative of events seen and accepted by public opinion. This capability will enable the priming and/or shaping of public opinion to make it susceptible to US strategic messaging. Once primed, just as the pebble can either turn a smooth river into turbulent white water or direct the water slightly more left or right, so will this new form of influence operate.

Influence campaigns have already been successfully employed by our adversaries.[11] The US has been a cultural goliath since the rise of Hollywood. Now is the time for the US to leverage its dominance in the realm of ideas and transform its operational paradigm to incorporate those skills and abilities. IIOs can leverage that dominance either directly through contracting with advertising and marketing firms to create specifically targeted content, or indirectly by utilizing advertisement targeting, search engine optimization, or targeted latency. These indirect effects would allow us to effectively guide perception and even shape the targeted population's perception of reality, if effectively conducted. The ability to control a population's perception will be a critical capability in ascertaining the shape of future events and determining how actions are perceived. IIOs will be the fusion of cyberspace operations and strategic messaging.

OVERT IMPACT

In the cyber realm, the soft, unnoticed touch can be massively more impactful than the forceful haymaker. An example of an overt impact is when Amazon Inc. lost over $72 million in sales as Amazon.com went down for 63 minutes during Prime Day in 2018, a loss of over $1 million per minute.[12] Conversely, "cart abandonment," (the industry term for not completing the checkout process after adding items to an online shopping cart) due to latency, cost the e-commerce industry approximately $18 billion in 2019.[13] A 2013 study showed minor increases in latency, on the order of two seconds, increased cart abandonment rates by 30%.[14] Two seconds became the difference between a successful sale and a lost opportunity. While the cost per minute was greater during the Amazon outage, losses due to latency have had more than 200 times the impact annually. Such losses are insidious, hard to attribute, and even more difficult to fix. The fact that such minor changes in availability have such an outsized effect shows how susceptible the impatient public is to minor inconveniences.

OPERATIONALIZING IIOS

There are multiple options for making IIO's a reality. The most direct method is to take ad-

vantage of the public's need for information on demand. Even DISA defines "extreme" latency as 100ms (one tenth of a second) above normal in Mission Partner Service Level Agreements (SLAs). To take advantage of this impatience, operators need to find ways to inject a relatively small amount of lag in targeting information sources. This would be best done through indirect means such as slowing down referenced style scripts, adding slight increases to traffic (aka a low-level D/DOS, enough to slow slightly down services, but not take them down), or working at the transport layer to increase lag at key points in the routing architecture. Once that lag is in place, the operations simply need to follow up with well-targeted advertisements to offer alternative information sources. These alternative sources will have the preferred narrative that the operation seeks to advance. There is little brand loyalty in the online world. Consumers will go elsewhere to find what they need if their preference is slow or unavailable. Influencing and controlling that "someplace else" yields the opportunity to wield influence. This is possible without a great emphasis on content creation; it just requires the preferred viewpoint to be amplified and the targeted one to be dampened.

When conducted effectively, IIOs can be exceedingly powerful; however they will need to be employed in support of strong consistent national objectives to be truly effective. While IIOs can certainly be used in a short-term targeted manner, they would best be employed for long-term operations executed over the course of years to help guide long-term changes in perceptions towards US interests and preferred global structure.

IIOs need to be closely governed to ensure that, although they influence global perceptions, their impact upon domestic populations must be limited or governed appropriately. That is not to say domestic IIOs cannot be conducted, but they need to be conducted with a very different aim. The aim of domestic IIOs should be to ensure that adversarial IIOs are ineffective. This can be accomplished by utilizing news fatigue effects, exposure to more divergent views to break senses of consensus, or directly reducing the viewing of an adversary's IIO content.

CONCLUSION

IIOs offer a huge potential for advancing cyberspace operations that support US national interests without the need for large-scale deployments or use of critical offensive cyber operations capability for smaller-gain operations. However, IIOs will require a wider and longer world view for optimal employment.

IIOs represent the operationalization of cyberspace to exert influence. They provide the ability to target and influence incredibly specific, or broad, populations with targeted messaging. This influence expands the US capability to exert soft power. This soft power, represented by Information Influence Operations, facilitates economy of force in the cyber realm. Not every problem can or should be solved with force, whether that force is physical or virtual. IIOs represent the alternative. IIOs are a critical tool to be advanced by USCYBERCOM as it develops its messaging capability in the cyber domain.

DISCLAIMER

The views expressed in this work are those of the author(s) and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense.

NOTES

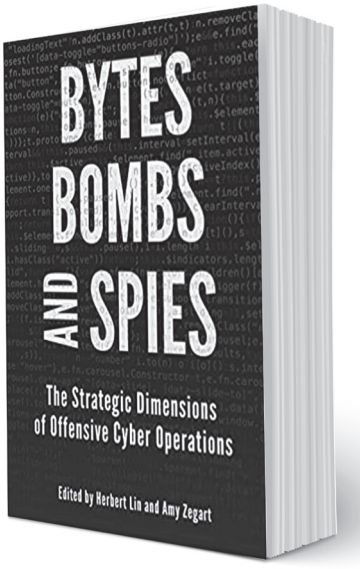
1. Lauren C. Williams, "Fogarty has Big Ambitions for ARCYBER." Last modified August 7, 2018, https://defensesystems.com/articles/2018/08/07/arcyber-priorities-williams.aspx.
2. Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, Washington, DC: United States Department of Justice, 2019), 4.
3. Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." Last modified November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.
4. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." Last modified August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
5. Mueller, 2018, 4.
6. Bob Franklin and Lily Canter, "Digital War Reporting," *Digital Journalism Studies: The Key Concepts.* (New York: Routledge, 2019).
7. "Mission Statement," British Broadcasting Corporation (BBC), accessed February 2, 2020, https://www.bbc.com/aboutthebbc/governance/mission.
8. "BBC Report: Trust and Impartiality Nov 2017," Trust Report, British Broadcasting Corporation (BBC), last modified November 2017. https://downloads.bbc.co.uk/aboutthebbc/insidethebbc/howwework/reports/pdf/bbc_report_trust_and_impartiality_nov_2017.pdf.
9. "About Us," Mission Statement, Russia Today, accessed February 2, 2020, https://www.rt.com/about-us/.
10. "Seven Commandments of Fake News – New York Times exposes Kremlin's methods," EU vs. DisInfo, European External Action Service (EEAS), last modified November 21, 2018. https://euvsdisinfo.eu/seven-commandments-of-fake-news-new-york-times-exposes-kremlins-methods/.
11. Mueller, 2018, 4.
12. Allison Enright, "The Potential Cost of Amazon's Prime Day Miss: 72 Million," last modified July 17, 2018, https://www.digitalcommerce360.com/2018/07/17/the-potential-cost-of-amazons-prime-day-miss-72-million/.
13. Design Advisor. "Shopping Cart Abandonment Stats." Last modified March 25, 2019. https://designadvisor.net/blog/shopping-cart-abandonment-stats/.
14. Tammy Everts, "Case Study: Slow Load Times Shopping Cart Abandonment," last modified October 31, 2013, https://blog.radware.com/applicationdelivery/applicationaccelerationoptimization/2013/10/case-study-slow-load-times-shopping-cart-abandonment/.

The Cyber Defense Review

BOOK REVIEW

Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations

Edited by Herbert Lin and Amy Zegart



Reviewed by
Cadet Annalise Callaghan
Dr. Jan Kallberg

EXECUTIVE SUMMARY

The following book review explores the content and insights of Dr. Herbert Lin and Dr. Amy Zegart's *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*. Initially published in 2018, the book is composed of a collection of works by prominent cyber scholars, practitioners, and professionals on the strategic uses of offensive cyber operations. This review begins with a contextualization of the circumstances that inspired the editors to convene the featured experts to collaborate on the book with the ultimate goal of filling the critical gap in conceptual thinking that has, to date, lagged behind the development and engineering of cyber technologies. The review proceeds by sorting the book's works into four interrelated themes pertaining to offensive cyber operations: (1) strategy and doctrine, (2) operational considerations, (3) escalation dynamics and deterrence, and (4) the role and relationship of the private sector. These subsections attempt to identify the book's variety of authors' academic and professional backgrounds – the diversity in these backgrounds and the prevalence of not only academic tenure but also practical experience serve as one of the book's unique strengthening characteristics. Within each theme, the review then provides a synopsis of the authors' various analyses in their respective works. The book that emerges as a product of these analyses and contributions traverses new territory in cyberspace thinking, addressing the strategic cyber landscape's fundamental technical, political, historical, psychological, and legal dimensions. Accordingly, *Bytes, Bombs, and Spies* is a text worthy of a hall of fame certification.

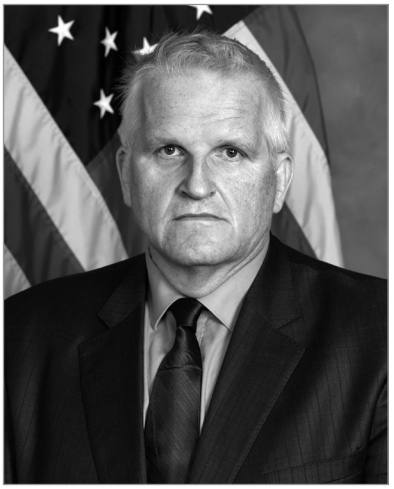
This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.

Cadet Annalise Callaghan is a yearling at the United States Military Academy. She is a double major in International Affairs and Law and Legal Studies: her research focuses include politics and power in cyberspace, information warfare, political participation, international cyber law, and privacy law. She is a Dean's Writing Fellow; serves on the officer teams of the West Point Ethics Debate Team and Ski Patrol; and is a participating member of the Parliamentary Speech and Debate Team, Model United Nations, the Domestic Affairs Forum, the International Affairs Forum, the Civic Engagement Initiative, and the Student Council on United States Affairs, along with several cultural and diversity forums. CDT Callaghan is originally from Eagle River, WI, and Houghton, MI. Upon graduation, she hopes to branch Cyber or Military Intelligence.

REVIEW

It was 2008 when centrifuges first began to malfunction at the nuclear facility in Natanz, Iran. The plant employees were perplexed when control room records indicated business as usual – none of the signals pointed to equipment failure. Some were fired; others were physically staged to oversee centrifuge performance and report their observations. Stands of linked centrifuges were carted away under suspicions of poor engineering, incompetence, and sabotage. It was not until two years later that the culprit – a computer worm that quickly became known as Stuxnet – accidentally emerged on the global stage. In the weeks that followed the computer worm's initial discovery, several new variants were directed at the Iranian nuclear plant in Natanz at close intervals, culminating with the temporary impairment of nearly one-fifth of the facility's nuclear centrifuges. The exposure and emergence of what can be considered the world's first significant cyber weapon and the engineering of its deployment (at least in part) by US forces would have profound implications for the decade that was to follow. Today, the utilization of Stuxnet by US and Israeli forces in Operation Olympic Games is widely credited with the slowing of Iran's progress toward the generation of a nuclear weapon: the extent to which it truly did so – and the questions regarding the operation's broader impact on US political and strategic power – remain.

One of the most notable aspects of Stuxnet's emergence was its reflection of the increasingly prominent roles that offensive cyber operations were coming to play in both US policy and international security. In the years following its discovery, however, the necessity of conceptual thinking to realize and articulate the effects of offensive cyber operations on the world was all but ignored. This fundamental gap in the literature on cyberspace served as the impetus for Dr. Lin and Dr. Zegart – Senior Fellows at Stanford University's Center for International Security and Cooperation – to host a



Dr. Jan Kallberg is Assistant Professor of American Politics in the Department of Social Sciences and Cyber Policy Fellow at the Army Cyber Institute at West Point. He holds a Ph.D. in Public Affairs and a Master's Degree in Political Science from the University of Texas at Dallas, and a J.D./LL.M. from Stockholm University. Prior to joining the West Point faculty, Jan was a researcher and Post-Doc at the Cyber Security Research and Education Institute, Erik Jonsson School of Engineering and Computer Science, at the University of Texas at Dallas under Dr. Bhavani Thuraisingham. Dr. Kallberg's research interest is the intersection between public leadership and cyber capabilities, especially offensive cyber operations as an alternative policy option. His personal website is www.cyberdefense.com.

research workshop at Stanford in 2016, uniting distinguished researchers and professionals from the US military, intelligence, and policymaking communities to illuminate the critical dimensions of offensive cyber operations. They deliver the culmination of that collective effort in the book *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations.* The chapters in the volume underscore the emergence of four interrelated themes regarding offensive cyber operations: (1) strategy and doctrine, (2) operational considerations, (3) escalation dynamics and deterrence, and (4) the role and relationship of the private sector. In doing so, the book significantly advances the literature on the technical, political, historical, and legal dimensions of offensive cyber operations.

The first thematic category of the book is introduced by Chris Inglis, the former Deputy Director of the National Security Agency. In his segment, he identifies the roles of intelligence, surveillance, and reconnaissance in cyberspace, arguing that the need for persistence in all three categories is both operationally justified and constrained by legal and structural factors of society. He underscores the challenge of ambiguity in cyberspace, particularly concerning intent, and elaborates on how domestic and international law can necessitate restraint in military operations. Inglis concludes by providing recommendations for measures that can be taken by government departments and agencies to reconcile conflicting goals in the cyber domain while improving the overall intrinsic power of intelligence, surveillance, and reconnaissance efforts. Inglis is followed by George Washington University professors Henry Farrell and Charles L. Glaser (a former member of the Pentagon's Joint Staff), who explain how effects, saliencies, and norms should influence US cyberwar doctrine. They argue that understanding the focal points of adversaries is critical to anticipating their interpretations of offensive cyber operations by the US. They go further by demonstrating the implications this

premise has for diplomatic potential and cyber policy development. Dr. Max Smeets and Dr. Lin follow this analysis with an overview of U.S. Cyber Command (USCYBERCOM) strategy and recommendations for enhancing command capabilities, emphasizing the importance of prioritization and operational speed. Their scenario-based analysis of the command's strategy provides a compelling framework for the analysis of the potential outcomes it may yield. These three subsections provide comprehensive insight into the roles and impacts of strategy and doctrine in offensive cyber operations.

Dr. Austin Long, a Senior Political Scientist at the RAND Corporation, initiates the book's discussion on the operational considerations of offense in cyberspace. He contemplates the circumstances in which strategic influence can constitute a strategic attack in cyberspace and employs analysis of nuclear planning processes to frame his approaches to organizational planning, execution, and deterrence. The U.S. Naval Academy Keyser Chair of Cybersecurity Studies, Dr. Martin Libicki, builds upon the conversation by pointing out that adversaries are likely to learn from and adapt to US-based cyber operations: the effectiveness of secondary operations, he argues, is a function of how well initial operations can be designed to mitigate opportunities for enemy adaptation. Dr. Lin provides a survey of possible approaches to hacking a foreign adversary's missile development program. Long, Libicki, and Lin's respective works yield important deductions regarding the design, organization, and execution of major operations in cyberspace, especially when those operations pursue specific strategic goals.

Six chapters of Lin and Zegart's book are dedicated to the theory and analysis of escalation dynamics and deterrence in cyberspace. Discussion of these themes is grounded by five types of escalatory pressures: intelligence collection, commingling of assets for command and control, inappropriate rules of engagement and scope, public opinion, and unintended damage. Jason Healey – the Founding Director for Cyber Issues at the Atlantic Council – begins this discussion by pointing out that cyber conflict is often more escalatory than deterrent. With special emphasis on the Iranian response to Stuxnet, several case studies identify the security dilemma inherent to states' behavior as they perpetually work to increase their respective cyber capabilities. Erik Gartzke and Jon Lindsay also subscribe to this view, adding distinctions between cyber operations directed towards counterproliferation and preemptive counterforce, along with the insight that offensive cyber operations against nuclear weapons systems raise the risk of nuclear war. The following chapter reports on research – conducted by Michael Gross, Daphna Canetti, and Dana Vashdi – regarding the psychological harms and negative impacts of offensive cyber on attitudes and opinions – specifically on public confidence in national institutions. Steven Bellovin, Susan Landau, and Herbert Lin follow this by articulating the fact that appropriate intelligence can yield possibilities for discriminatory cyber-attacks: in other words, operations that limit damage to their targets. The twelfth chapter of the book, written by Michael Sulmeyer, C. Robert Kehler, and Herbert Lin, expounds upon the legal constraints identified by Chris Inglis at the beginning of the book, identifying the characteristics of operations in cyberspace that complicate the formulation of policy and rules of engagement.

Adam Segal draws upon these five chapters to compose a prospective case study addressing the potential for cyber escalation in a military confrontation between the US and China.

The fifteenth and sixteenth chapters of this book come to opposite conclusions regarding the private sector's role in offensive cyber operations. While David Aucsmith argues for the necessity of legal reform that would enable private companies to take offensive action consistent with the law of armed conflict, Lucas Kello contends that the capacity of such private action to upset international conflict stability and to put innocent third parties at risk constitutes too great a danger to be ignored. Irv Lachow and Taylor Grossman conclude the book with an objective overview of the private sector's role in supporting offensive cyber operations in government.

CONCLUSION

Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations fills critical gaps in the literature on offensive cyber operations to date, addressing fundamental technical, political, psychological, and legal dimensions of the strategic cyber landscape. The book's strength is underscored by its diversity of perspective and analysis by esteemed researchers and academics in the field, among whom professional experience working in government and security-related positions is notably prevalent. The book's internal validity is enhanced by the interconnectedness of arguments that fall under different themes, though it occasionally misses opportunities to substantively discuss contradictions between the array of theoretical frameworks it espouses. Frameworks for determining and measuring the effectiveness of offensive cyber operations constitute a critical gap in the literature, and should be pursued in future research. Despite the applicability of the literature in this book to the Stuxnet case study, for instance, the weapon's ultimate effectiveness is its most hotly debated and contested variable. It is also the one that poses the most significant strategic, ethical, political, and legal questions concerning the future offensive cyber operations. Defining a framework for the measurement of operational effectiveness has the potential to inform offensive cyber strategy – and subsequently, to influence cyber effects – for generations to come. The knowledge and analysis provided in *Bytes, Bombs, and Spies* contributes to the necessary foundation for such an endeavor to be pursued.

Title: ***Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations***
Publisher: Brookings Institution Press (January 15, 2019)
Paperback: 426 pages
Language: English
Paperback ISBN 978-0-8157-3547-2
Ebook ISBN 978-0-8157-3548-9
Price: $45.99 Paperback
$19.79 Kindle Edition

THE CYBER DEFENSE REVIEW

CONTINUE THE CONVERSATION ONLINE

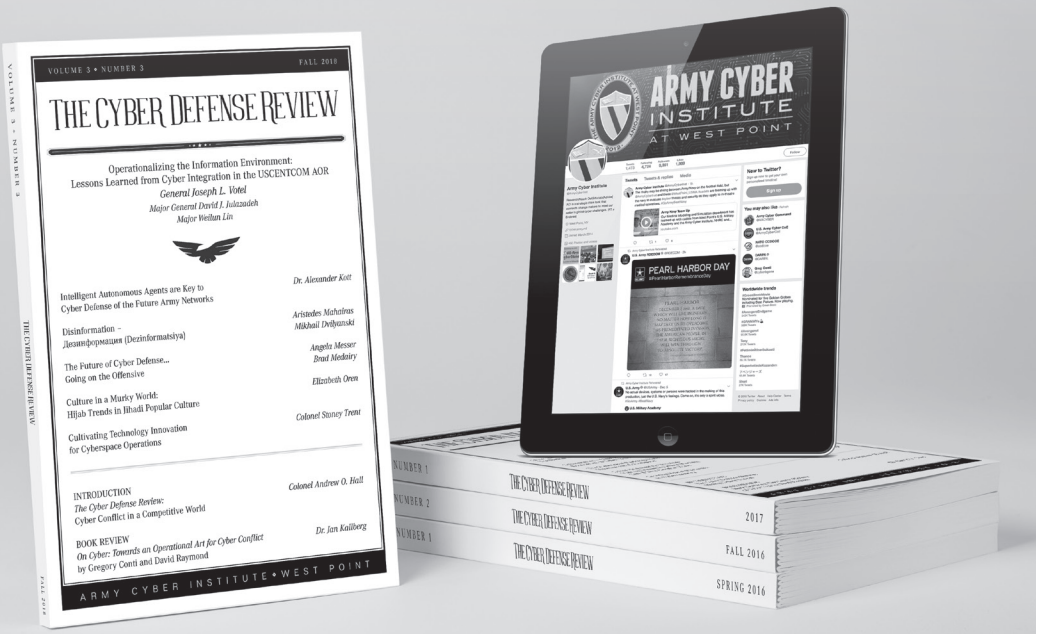
CyberDefenseReview.Army.mil

AND THROUGH SOCIAL MEDIA

Facebook @ArmyCyberInstitute

LinkedIn @LinkedInGroup

Twitter @ArmyCyberInst
@CyberDefReview



ARMY CYBER INSTITUTE • WEST POINT

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