

THE CYBER DEFENSE REVIEW

Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack

The Honorable Joe R. Reeder

Cadet Tommy Hall



Cybered Competition, Cooperation, and Conflict
in a Game of Imperfect Information

Hiram Henderson

China's Arctic Cyber Espionage

Emilio Iasiello

Attack-Based Network Defense

Maj. William North

Technology Adoption in Unconventional Warfare

Sean W. Pascoli
Dr. Mark Grzegorzewski

RT and the Element of Disguise:
Russia's Information Weapon

Tobias Redington

Combined Information Overlay for Situational
Awareness in the Digital-Anthropological Terrain

Dr. Zac Rogers
Dr. Emily Bienvenue

Risks to the Mission Partner Environment:
Adversarial Access to Host Nation Network Infrastructure

Capt. Kyle Sullivan

INTRODUCTION

Ransomware's Growing Impact

Col. Jeffrey M. Erickson

BOOK REVIEW

*Outsourcing War to Machines:
The Military Robotics Revolution*
By Paul J. Springer

Cadet Dylan Taylor
Maj. Mark Lesak

THE CYBER DEFENSE REVIEW

◆ SUMMER EDITION ◆

THE CYBER DEFENSE REVIEW

A DYNAMIC MULTIDISCIPLINARY DIALOGUE

EDITOR IN CHIEF

Dr. Corvin J. Connolly

MANAGING EDITOR

Dr. Jan Kallberg

ASSISTANT EDITORS

West Point Class of '70

ARMY CYBER INSTITUTE

Col. Jeffrey M. Erickson
Director

Dr. Paul Maxwell
Deputy Director

Sgt. Maj. Amanda Draeger
Sergeant Major

Dr. Edward Sobieski
Senior Faculty Member

Col. Stephen S. Hamilton, Ph.D.
Chief of Staff

CW4 Jancee L. Potts, Ph.D.
Chief Warrant Officer

AREA EDITORS

Dr. Harold J. Arata III
(Cybersecurity Strategy)

Dr. Steve Henderson
(Data Mining/Machine Learning)

Dr. David Raymond
(Network Security)

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

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

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

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

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

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

Dr. David Gioe
(History/Intelligence Community)

Dr. Fernando Maymi
(Cyber Curricula/Autonomous Platforms)

Dr. David Thomson
(Cryptographic Processes/Information Theory)

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

Dr. William Clay Moody
(Software Development)

Dr. Robert Thomson
(Learning Algorithms/Computational Modeling)

Dr. Dawn Dunkerley Goss
(Cybersecurity Optimization/Operationalization)

Dr. Jeffrey Morris
(Quantum Information/Talent Management)

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

Dr. Michael Grimaila
(Systems Engineering/Information Assurance)

Ms. Elizabeth Oren
(Cultural Studies)

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

EDITORIAL BOARD

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

Dr. Martin Libicki
U.S. Naval Academy

Dr. Bhavani Thuraisingham
The University of Texas at Dallas

Dr. Amy Apon
Clemson University

Dr. Michele L. Malvesti
Financial Integrity Network

Ms. Liis Vihul
Cyber Law International

Dr. Chris Arney
U.S. Military Academy

Dr. Milton Mueller
Georgia Tech School of Public Policy

Prof. Tim Watson
University of Warwick, UK

Dr. David Brumley
Carnegie Mellon University

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

Prof. Samuel White
Army War College

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

Dr. Hy S. Rothstein
Naval Postgraduate School

CREATIVE DIRECTORS

Sergio Analco | Gina Daschbach

LEGAL REVIEW

Courtney Gordon-Tennant, Esq.

KEY CONTRIBUTORS

Clare Blackmon

Kate Brown

Erik Dean

Col. Michael Jackson

Alfred Pacenza

Michelle Marie Wallace

Nataliya Brantly

Neyda Castillo

Debra Giannetto

Lance Latimer

Diane Peluso

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

Col. Jeffrey M. Erickson

9

*The Cyber Defense Review:
Ransomware's Growing Impact*

SENIOR LEADER PERSPECTIVE

**The Honorable Joe R. Reeder
Cadet Tommy Hall**

15

*Cybersecurity's Pearl Harbor Moment:
Lessons Learned from the Colonial
Pipeline Ransomware Attack*

RESEARCH ARTICLES

Hiram Henderson

43

*Cybered Competition, Cooperation, and
Conflict Game of Imperfect Information*

**Sean W. Pascoli
Dr. Mark Grzegorzewski**

61

*Technology Adoption in
Unconventional Warfare*

Tobias Redington

75

*RT and the Element of Disguise:
Russia's Information Weapon*

**Dr. Zac Rogers
Dr. Emily Bienvenue**

89

*Combined Information Overlay
for Situational Awareness in the
Digital-Anthropological Terrain:
Reclaiming 'Information' for
the Warfighter*

Capt. Kyle Sullivan

109

*Risks to the Mission Partner
Environment: Adversarial Access
to Host Nation Network Infrastructure*

RESEARCH NOTES

Emilio Iasiello	121	China's Arctic Cyber Espionage
Maj. William North	129	Attack-Based Network Defense

BOOK REVIEW

Cadet Dylan Taylor Maj. Mark Lesak	141	<i>Outsourcing War to Machines: The Military Robotics Revolution</i> By Paul J. Springer
---	-----	---

THE CYBER DEFENSE REVIEW

◆ INTRODUCTION ◆

VOL. 6 ♦ NO. 3

The Cyber Defense Review: Ransomware's Growing Impact

Colonel Jeffrey M. Erickson



Welcome to the Summer 2021 edition of *The Cyber Defense Review* (CDR) where you will find a collection of thought-provoking articles in this issue.

First, let us start with the elephant in the room: Ransomware. Ransomware has become a household name over the last year, with the frequency and scale of the attacks increasing at an alarming rate. We hear almost weekly of a significant attack affecting multiple organizations, both as primary targets and as downstream collateral targets. The recent Colonial Pipeline shutdown and JBS's meat processing plant disruptions demonstrated in very real terms the potential impacts of cyberattacks on large portions of the American population. Clearly, the status quo is not working.

To address this issue, the Honorable Joe R. Reeder (former Under Secretary of the Army) and United States Military Academy (USMA) Cadet Tommy Hall assess the implications of the Colonial Pipeline event and provide seven key lessons that the Nation must address in their article: "Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack."

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



Colonel 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.

While ransomware is receiving most of the media's attention, our authors are also looking at other concerning trends and potential vulnerabilities worth considering:

- ◆ **Supply Chain Vulnerabilities:** Captain Kyle Sullivan asks the very pertinent question: Is the Mission Partner Environment (MPE) at risk due to equipment manufactured by possible adversaries? If you have concerns about NATO's ability to achieve the Federated Mission Network (FMN) and the United States' initiative to support it, you will find the article, "Risks to the Mission Partner Environment: Adversarial Access to Host Nation Network Infrastructure," riveting.
- ◆ **Russian Information Warfare:** Tobias Redington's article "RT and the Element of Disguise: Russia's Information Weapon," highlights RT's tactics and techniques to build legitimacy while practicing deception and mis/disinformation. He highlights examples of the dishonest behavior and mis-directions of this organization and its success in simultaneously building a global audience. His article is a call to action for Western governments and provides some possible options.
- ◆ **China's Approach to the Arctic:** The Arctic is continuing to become a focus for future defense-related issues. In his article, "China Arctic Cyber Espionage," Emilio Iasiello assesses China's approach to the region, through investment, mineral rights, and cyber espionage. Could this be setting the stage for a "Polar Silk Road?"

Additionally, many of our authors propose new approaches to build capability, see ourselves, and approach complex problems:

- ◆ **Unconventional Warfare:** In the article, "Technology Adoption in Unconventional Warfare," Sean Pascoli and Dr. Mark Grzegorzewski propose using the model of irregular and non-traditional forces

with cyber capabilities. Using methods such as employing cyber-capable irregular forces and cyber-proxies to deny infrastructure and networks to adversaries while enabling access to allies. As they aptly point out: how do we change the risk aversion mindset that enables proxies to conduct kinetic operations, yet will not enable actions in the cyber domain? Using the Seven Phases of Unconventional Warfare, they describe some of the actions UW forces could employ to support larger operations and strategic objectives.

- ◆ **Game Theory:** Hiram Henderson recommends the use of game theory to enable the Joint planning process in his article “Cybered Competition, Cooperation, and Conflict in a Game of Imperfect Information.” Drawing from the lessons learned from nuclear deterrence, he provides some thoughts and planning considerations for a cyber-based approach.
- ◆ **Enhancing PMESII:** In their article, “Combined Information Overlay for Situational Awareness in the Digital-Anthropological Terrain: Reclaiming ‘Information’ for the Warfighter,” Dr. Zac Rogers and Dr. Emily Bienvenue provide a construct that combines the familiar PMESII-PT (political, military, economic, social, information, infrastructure, physical environment, and time) taxonomy with the lesser-known Digital Anthropological Terrain (DAT) construct in a structured manner to inform decision-makers, and subsequently translate intent into action.
- ◆ **Cataloging Threats:** In “Attack-Based Network Defense,” Major William North proposes the adoption of a standardized and quantifiable methodology to catalog known and unknown threat techniques to allow for better training, testing, synchronization, and incident response.

For those interested in expanding their understanding of artificial intelligence and robotics with respect to warfare, USMA Cadet Dylan Taylor and ACI’s Major Mark Lesak have provided a book review of Paul J. Springer’s *Outsourcing War to Machines: The Military Robotics Revolution*. They highlight the use of examples from the history of warfare and the revolutions in military affairs as they relate to the future employment of these systems.

The CDR is fortunate to have the brilliant design team of Sergio Analco and Gina Daschbach and world-class editors in Michelle Wallace, Dr. Jeff Morris, Courtney Gordon-Tennant, and LTC Mark Visger supporting the journal. The West Point Class of ’70 Assistant Editors: Hon. Joe R. Reeder, Dr. Bill Spracher, Chip Leonard, and Dr. Bill Lane enhance every CDR article with their thought leadership and scholarly engagement. Again, thanks for joining us for the Summer issue, and we look forward to continuing the discussion on these topics through active engagement in the wider cyber community.📧

THE CYBER DEFENSE REVIEW

◆ SENIOR LEADER PERSPECTIVE ◆

Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack

The Honorable Joe R. Reeder
Cadet Tommy Hall

INTRODUCTION

In 2014, former NSA Deputy Director Chris Inglis prophetically observed that “if we were to score cyber the way we score soccer, the tally would be 462-456 twenty minutes into the game, i.e., all offense.”^[1] Recent events demonstrate that Inglis’ warning is more urgent than ever, because our cyber defenses remain woefully inadequate. *The Washington Post* titled a feature article on July 11, 2021: “Would the US really answer cyberattacks with nuclear weapons?”^[2] Even to broach this question would prompt a follow-up: Has the US undertaken every practicable effort it can make to insulate its assets from cyberattacks? The discussion below explains why the answer is a resounding “No.”

On May 6, 2021, Colonial Pipeline was attacked by ransomware suspected to have originated in Eastern Europe or Russia,^[3] allowing cyber criminals to penetrate a major utility with significant impact on the entire US eastern seaboard’s economy. From the perspective of vulnerability, the Colonial Pipeline attack was a significant wake-up call—a Pearl Harbor moment for cybersecurity. Although Federal authorities eventually recovered \$2.3 of the \$4.3 million ransom paid, the DarkSide hacking group still gouged a seven-figure bitcoin profit. Headline news reported panic, social disruption, and a crippling lack of fuel delivery. This and other recent attacks referenced below highlight a serious and growing threat to national security. As such, this article discusses two related issues: (1) how much, and how, we as a nation must move to improve cyber defenses for critical infrastructure, and (2) some of the lessons we must apply to protect against increasingly disruptive cyber threats, with special focus on three aspects of cyber-security: protection and prevention, resilience and recovery, and deterrence. As facts (and attacks) continue to unfold, each of these areas can and should be the focus of deeper analysis.

The contribution of Cadet Tommy Hall is the work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.
© 2021 Joe R. Reeder



Joe R. Reeder, a 1970 West Point graduate and 82nd Airborne Division soldier, served as the Army's 14th Under Secretary and Chairman of the Panama Canal Commission (1993-97). For the past 23 years he has been a leader and senior shareholder in one of the world's largest international law firms, Greenberg Traurig, LLP, with clients including public figures, entertainers, and nations.

As a general proposition, the Department of Homeland Security (DHS) orients much more toward cyber defense, while the Department of Defense (DoD) provides cyber offense. Yet our overall national policy remains quite uncoordinated, with several cyber “stovepipes” that have separate authorities and missions, for example: DHS, Department of Justice (DOJ)/Federal Bureau of Investigation (FBI), DoD/US Cyber Command (CYBERCOM), NSA/Intelligence Community (IC). These stovepipes render coordination ad hoc at best, and more reactionary to cyber events as they arise. The FY21 National Defense Authorization Act (NDAA) created a National Cyber Director to help correct this weakness, but time now is of the essence.

A Brief History of Ransomware Attacks in the United States

On Friday, May 7, 2021, at 5:00 AM, a Colonial Pipeline employee found an electronic ransom note demanding millions of dollars in cryptocurrency.^[4] Within seventy minutes of this discovery, Colonial Pipeline shut down all 5,500 miles of its pipelines.^[5] On June 2, 2021, employees at JBS USA Holdings, Inc., one of the world's largest meat companies and a major beef supplier in the US, awoke to find a similar message. The CEO made the tough decision to pay \$11 million in ransom.^[6] Less than a day later, the ferry service that shuttles sightseers to Martha's Vineyard met the same fate. Along these same lines, even a global pandemic did not deter malicious actors from targeting facets of everyday life, from tourism to lifesaving medicines.^[7]

While it is partially true that ransomware hackers began with low-profile targets and grew bolder over time, public health researchers may have been the first ransomware victims. In 1989, Joseph Popp, a Harvard-educated evolutionary biologist, delivered floppy disks to twenty thousand researchers worldwide that purported to include an informational program pertaining to AIDS.^[8] This elaborate ruse succeeded in infiltrating researchers' networks and encrypting their files, and



Tommy Hall, a West Point senior, focuses his research on China, including how historical concepts of nationalism influences contemporary interstate relations, domestic politics, and Communist Party legitimacy. His other interests include US cybersecurity, refugees, and human rights policies. As a Stamps Scholar, Chinese language major, and West Point policy debater, Cadet Hall hopes to use his expertise to build diverse, interdisciplinary teams willing to tackle the complex challenges that intersect national security and human rights in the 21st century.

Popp's floppy disks demanded a fee for decryption. These initial ransomware attacks amounted to urgent messages and encrypted files in exchange for money, or "scareware" that bombarded computers with pop-ups and urgent messages such as "SECURITY WARNING!"^[9] Computer operator victims, upon closing the warnings, found their files encrypted. The goal of such pioneer ransomware hacks mirrors the Colonial Pipeline attacker's: strangle the victim until it pays the ransom to unlock captive files.

Ransomware has become increasingly common and hard to defend against. Ransomware attackers can look for any vulnerability across a vast array of targets, exploit it, and extract a ransom. This general strategy is what makes ransomware, at its core, an opportunistic attack. Effectively thwarting it requires either defending every target (an unworkable solution) or undercutting the business model itself by exponentially raising financial costs. The US Government (USG) faces similar challenges with general cybersecurity. What is different with ransomware is that it is intentionally disruptive – a far cry from traditional attacks that prioritize stealthy and long-term network penetrations over all other considerations.

Both the number and magnitude of ransomware demands have exploded over the past decade. In 2015, the FBI estimated the US suffered a thousand daily ransomware attacks, a statistic that quadrupled by 2016^[10]. A December 2019 USG report cited nearly a thousand ransomware attacks targeting a range of victims, from pipelines to schools to hospitals.^[11] Accurate statistics on ransomware and other cyber-attacks remain elusive, in part due to lack of any standardized statistics that consolidate existing estimates, and, because, as discussed more fully below, the US is yet to commit to a nationwide, collective "buy-in" to the benefits of real-time reporting and cooperation with government cyber institutions. Similar to Dr. Anthony Fauci's efforts to motivate 100 percent COVID-19 vaccinations, catalyzing

CYBERSECURITY'S PEARL HARBOR MOMENT

cybersecurity “buy-in” is essential. By some accounts, literally millions of ransomware attacks go unreported, but these estimates vary wildly and many are based on one-off, educated guesses at best. See for example, Figure 1 below, which reports the number of global ransomware attacks during 2020 at 304.6 million.^[13]

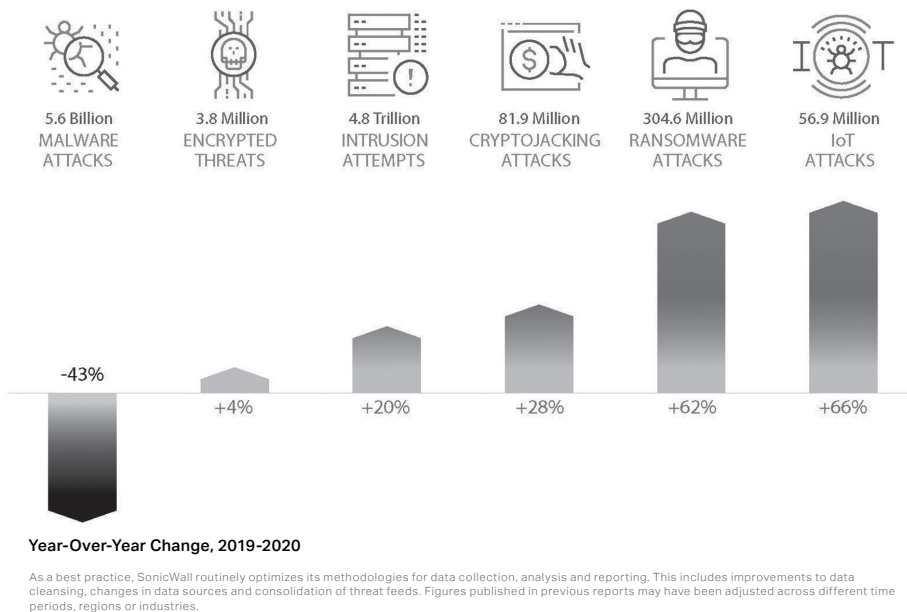


Figure 1. 2020 Global Cyberattack Trends Report by SonicWall

Without granulating based on the size of the victimized business, the average of all ransom demands by one account grew from a few thousand dollars in 2018 to \$200,000 in 2020.^[14] Hacker methods also have become far more sophisticated and often are timed to strike victims when they are most vulnerable and least able to survive interrupted operations (e.g., hitting schools in August and accounting firms during tax season).^[15] The global pandemic gave hackers a golden opportunity to inundate emergency services and struggling businesses. For example, the strike on Universal Health Services and its chain of over 400 hospitals, on September 27, 2020, was the largest-ever medical cyber-attack in the US. *The New York Times*'s top cyber expert, Nicole Perlroth, in her superbly researched book underscores the disturbing rise of cyberattacks experienced during the COVID-19 pandemic.^[16]

The White House has attributed the rapid expansion and professionalization of ransomware operations partly to cryptocurrencies' unregulated growth.^[17] Bitcoin and other cryptocurrencies, while highly volatile, enhance operational security for money-laundering and ransom pay-offs. Cryptocurrency facilitates ransomware operations by shielding exchanges not tied to or controlled by a central bank, thereby cloaking digital ransom payments in anonymity.^[18] Transactions are recorded on a public ledger but are not brokered by a middleman witness to the identity of either party.^[19] Nor are offshore cryptocurrency exchanges governed by

anti-money-laundering laws, such as the US “know your customer” (KYC) laws,^[20] that penalize those who facilitate financial transactions that facilitate crime.^[21]

Many, if not most, of the recent high-profile attacks against the US were perpetrated by Russia-linked cyber-criminal organizations, and cryptocurrencies help conceal them from US intelligence and law enforcement. While the Kremlin’s denials no longer seem plausible, Russia persists in fiercely denying any coordination, for example, with the DarkSide group or REvil. Whether or not our intelligence community still lacks conclusive proof as to any specific criminal, Eastern European- and Russian-based cyber-criminal syndicates continue to target US public and private entities with impunity and have yet to face meaningful repercussions.^[22]

Assessment of Critical Infrastructure Defense Progress

Not until 2018 did the DoD designate protecting “US critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a significant cyber incident,”^[23] as a top cyberspace priority. Presidential Policy Directive 41 (PPD-41) defined a significant cyber incident as one conducted through a computer network likely to harm national security, foreign relations, and/or the US economy, and its definition also includes threats to civil liberties, public confidence, and public health and safety of US citizens.^[24]

PPD-41 is a good start, but the US remains far short of its full potential to defend key infrastructure from crippling cyber-attacks, even after devoting a laudable, if not gargantuan, budget to this goal (\$17.4 billion spent on cybersecurity-related activities in FY2020 alone).^[25] The DoD has no statutory authority to “protect” critical domestic infrastructure, yet received \$8-10 billion of this total. About \$2 billion went to DHS’s Cybersecurity and Infrastructure Security Administration (CISA), the agency statutorily charged with assisting to protect domestic critical infrastructure. Wholly aside from the resource allocation, obviously more must be done to prevent novice^[26] criminals from being able to cripple the flow of gasoline over 5,000 miles of pipeline that supplies 45 percent of fuel along the entire East Coast for over a week.^[27] More sophisticated criminals mounted a multi-country assault that threatened our food supply with the JBS ransomware attack.^[28] Both Colonial Pipeline and JBS restored operations relatively quickly but not before paying multi-million dollar ransoms to criminals. These incidents also panicked millions of Americans and laid bare our nation’s stark vulnerability and lack of resilience.

In the June 8, 2021 hearing on the Colonial Pipeline attack, Chairman Gary Peters of the US Senate Committee on Homeland Security and Governmental Affairs reflected the fears of the American public and the defense community in his questioning of the company’s CEO: “Mr. Blount, I am glad your company continues to recover from this malicious attack and that the FBI was able to recover millions of dollars in ransom pay, but I am alarmed that this breach ever occurred in the first place and that communities from Texas to New York suffered as a result.”^[29] Mr. Blount explained that, “we responded swiftly to the attack itself and to the disruption that the attack caused ... We reached out to federal authorities within hours of the attack

and since that time we have found them to be true allies as we've worked quickly and safely to restore and secure our operations."^[30]

This exchange reveals two truths that the American public, the USG, and critical infrastructure owners must face. First, cybersecurity weaknesses continue to make our country's infrastructure vulnerable to attack. In our increasingly interconnected world, cybersecurity vulnerability manifests itself in more disruptive economic costs, to the point of posing a credible threat to national economic stability. Second, the best, and perhaps only, corrective actions will require effective, real-time collaboration, from ground-level analysts up to senior management, among federal, state, and local governments, and, equally importantly, with the full participation of our private sector. The private sector manages up to 85 percent of all critical US infrastructure,^[31] yet the bulk of the country's vital infrastructure does not receive the corporate and USG resources needed to defend against cyber criminals. That being stated, resources alone are not enough. Long-term success will require strong, focused USG leadership that is able to motivate a strong sense of urgency, and that provides clear and executable guidance, and collaboration with the private sector, characterized by genuine, two-way trust that rewards both sides with sharing of sensitive information in real time, specifically as to (a) strict adherence to basic cyber hygiene, (b) identification of all vulnerabilities,^[32] (c) reporting of attacks, (d) coordinated response to such attacks, and (e) prompt sharing of evolving best practices. Notwithstanding anonymity guarantees and limited liability protection, voluntary sharing thus far has failed. The key public policy question we now face is not whether to require the sharing of information (through reporting), but rather, how to require information, and from whom.

LESSONS THE NATION MUST TAKE TO HEART

1. Start with Adhering to Cybersecurity Basics.

While there are no silver-bullet solutions to ransomware, three basic cybersecurity ground rules must always be followed: (1) require multi- or two-factor authentication (2FA); (2) integrate segmentation into cyber systems; and (3) adhere to routine "patch-Tuesday" industry-standard practices.^[33] Sadly, Colonial Pipeline exemplifies one of many avoidable attacks in which the criminal organization exploited the company's lack of safeguards, specifically 2FA. While hardly a panacea safeguard against hacker penetration, 2FA would have prevented this one.^[34] Using a single password obtained from the dark web to log into a VPN account connected to Colonial Pipeline's network, DarkSide hackers exploited the absence of this basic 2FA cybersecurity must.^[35] One obvious lesson for Colonial Pipeline is clear: "Never again" violate any of the three cardinal hygiene basics.

In defending against malicious cyber-actors, both government and private sector players must adhere rigorously to all cybersecurity fundamentals. Along with embedding these cybersecurity basics, we also must establish simple digital literacy about commonly used network infiltration tactics for everyone having any role in protecting critical infrastructure.

Moreover, even after solid digital literacy and safeguards are in place, periodic audits and testing are essential.

Seasoned cyber experts also agree that most of China's and Russia's offensive cyber capabilities would die in the cradle if the US adhered to the three basic cybersecurity protocols.^[36] These protocols will help protect against not only less sophisticated, non-state-sponsored cyber-attacks, but also near-peer nations that are armed with some of the world's more advanced hacking capabilities. On what was a more sophisticated operation calling for the immediate shut down of servers, *The Washington Post* on July 3, 2021 reported what it termed the largest non-nation state supply-chain ransomware attack ever, affecting over hundreds of businesses using managed IT services. The hackers armed themselves with two different ransom notes that demanded \$50,000 of smaller firms and \$5 million from larger ones.^[37] This report also noted the rise of "hackers' band[ing] together and form[ing] cybercriminal gangs to extort...payment," gangs that begin by exploiting basic vulnerabilities before launching more sophisticated tactics.^[38]

2. Protect the Nation's Critical Infrastructure by Elevating the USG's Aspirational Private-Public Partnership (PPP) as a Top Priority.^[39]

Federal officials reportedly criticized Colonial Pipeline for not immediately involving CISA in post-attack investigation efforts,^[40] revealing problems with collaboration and information sharing between the USG and private firms.^[41] The roles and missions of the many involved USG agencies must be clarified so that infrastructure operators fully understand reporting protocols and ongoing collaboration.^[42]

In contrast to CISA's reported frustrations, other agencies applauded Colonial Pipeline's close coordination.^[43] On June 3, 2021, the DOJ formed the Ransomware and Digital Extortion Task Force in order to help centralize federal law enforcement efforts in combatting such cyber-attacks.^[44] Within days after its launch, this Task Force seized 63 of the 75 bitcoins Colonial Pipeline paid to DarkSide as ransom, recovering over \$2 million.^[45] JBS paid nearly three times that ransom with no funds yet recovered. The FBI attributes the 3-country JBS attack to REvil, a far more sophisticated ransomware hacker than DarkSide.^[46] Given the assets the USG can bring to bear, cyber-attacks almost always should trigger immediate federal agency reporting and cooperation.

Few seriously question the US prowess as a cyber trailblazer, but recent ransomware attacks demonstrate an abject failure so far to achieve critical private-public partnership (PPP) policy goals spelled out almost two decades ago in the National Strategy to Secure Cyberspace. This seminal cyber policy statement explained why protecting critical, Internet-connected infrastructure systems is impossible without a strong PPP.^[47] A decade later, the Obama administration adopted the framework now in use to enhance PPPs—a voluntary partnership model that enunciates overlapping but also distinct goals for commercial cybersecurity and national security.^[48]

The current voluntary PPP model continues to leave the US vulnerable, so the USG must consider complementing a better PPP with select mandated standards that appear to be working well for certain US allies. A good starting point might be to take a hard look at the insurance industry, that as of April 2021 was exposed to a \$1 trillion in cyber insurance policy limits.^[49] Unlike car insurance, cyber insurance thus far is voluntary. Making it mandatory, at least for certain critical companies, is a common sense step forward. The excellent, April 2021 Ransomware Task Force Report commissioned by the Institute for Security & Technology (IST) highlights the rapidly evolving role now played by privately placed cyber insurance. Less than 15% of global organizations have cyber insurance today, (including about 1/3 of all large US companies).^[50] About 20 of the largest insurers dominate this market, and the (a) rising premiums, (b) coverage restrictions, and (c) more stringent underwriting requirements in the marketplace are quite telling. In a very positive way, these changes can and should lead to seismic shift among companies exposed to ransomware in terms of investment and vigilance.^[51] In addition, some insurers have close connections with national and global law enforcement to facilitate the data-sharing and threat intelligence.^[52]

Nicole Perlroth notes that several of the world's more digitized countries seem nowhere near as vulnerable to cyber-attack as the US.^[53] She criticizes as wrong-headed US Chamber of Commerce lobbyists who complain that even voluntary standards are too onerous for private sector operators of our nation's critical infrastructure, and cites as proof several studies of the Scandinavian countries, Norway in particular (the world's fifth most digitized country), and Japan.^[54] She urges the need for laws with "real teeth" that, in addition to the three cyber hygiene basics, mandate immediate replacement of antiquated and/or unsupported software. Perlroth also commends Norway's annual revisit and update of its 2003 national cybersecurity strategy, noting that Japan does the same with its "remarkably detailed" cybersecurity policies first established in 2005.^[55]

Developing a much more integrated, effective PPP solution presents basic challenges, but none that are insurmountable. First, while profit-oriented private corporations are fully incentivized to pay what it takes to secure their own cyberinfrastructure, only the federal government can be expected to invest the time, effort, and resources that will secure the entire national security ecosystem, particularly against nation-sponsored adversaries. Vaughan Grant, former policy manager of the Australian Army's cyber operations, observed that "the social benefits derived from cybersecurity for critical infrastructure do not readily translate into economic benefits."^[56] Colonial Pipeline and JBS executives would probably agree that effectively safeguarding their operations with no governmental support would be cost-prohibitive. The public's cybersecurity needs obviously are not driven by the profitability of any one or more companies, which is why the federal government's role in the PPP team is essential.

Second, information sharing between private industries and the USG remains largely left up to private industry owner discretion.^[57] Absent company permission, USG agencies cannot

properly access network information to assist corporate efforts that lessen vulnerabilities to attack, and/or otherwise help respond post-attack.^[58] Again, what is now voluntary should become mandatory, with crystal clear ground rules as to what entities and what information must be reported, and to whom. Even if the USG worked much harder at the never-ending challenge of earning, and then holding, the trust of corporate America, “voluntary” may never work effectively. Nor do we have the luxury of time in which to experiment. The USG must take the lead, first by creating a clear and easily executable standard operating procedure with private sector partnership. The USG also must work to ensure that PPP “sharing” procedures do not compromise (a) security classifications, (b) competitive market realities, or (c) international laws. While due to US intelligence laws and not public-private information sharing, the mid-2020 European Court of Justice decision, Schrems II, invalidated the privacy shield after concluding that US law failed to protect data privacy.^[59] Finally, and as a further inducement for private sector involvement, the USG should provide incentives (e.g., liability protection for those entities that have satisfied certain standards), and other reasons to trust the USG. Otherwise, a tightly integrated level of real-time, meaningful information sharing will never happen.^[60]

The Obama administration in 2013 with E.O. 13636 groped with a fundamental challenge that still haunts the US—defining what constitutes truly critical infrastructure. Today eight years later, the definition of critical infrastructure has become so broad and unwieldy as to be meaningless. The Cyberspace Solarium Commission (CSC) sought to address this issue with the term Systematically Important Critical Infrastructure (SICI). Legislation is sorely needed to define this basic term. Lack of an accurate definition makes it literally impossible to determine the benefits to, and the burdens of such entities—benefits and burdens that also are in sore need of legislation. Also excluded in 2013 from E.O. 13636 was an effort to define was the IT sector. The devastating December 20, 2020, SolarWinds attack, has no doubt taught us that excluding IT as a protected SICI has left a glaring hole.^[61] The USG cannot work closely with all of the hundreds of thousands of US entities vulnerable to cyber-attack, the vast majority of which are not truly critical, but we do need to get the definition right in order to protect what is essential.

Without a disciplined, workable definition of SICI, PPP cybersecurity efforts today cannot begin to build the essential high level of trust and integrated cooperation necessary. So, at best, what we have is a piecemeal, post hoc division of labor once crises surface. At worst, but still better than nothing, vaguely drawn, uncoordinated “boundaries” exist with respective private-public players bumping into each other, dusting off, and walking away—two separate, uncoordinated entities facing a common enemy without any collective plan of defense. The US sometimes performs more optimally, but *always* must become the goal. To achieve that ideal, a solid PPP must be developed with all SICI’s, and it must extend well beyond pre-crisis agreement on respective responsibilities, to include collaborative exchanges from the bottom up in

each respective organization. The private sector can never shift all leadership responsibility to the federal government and then assume a passive “observer” status, because the first line of private-sector cybersecurity defense is, and will always be, the private sector that is privy to information no one in the USG has. Defense of critical infrastructure requires focus on highly collaborative and integrated *partnership*—the third of the three “Ps” in PPP. Serious leadership challenges face both partners: corporate leaders must be receptive towards the USG, and the USG must earn corporate confidence needed before gaining access to network and other highly sensitive commercial information. The USG can prove with the reward of success why private sector players should feel highly incentivized to collaborate fully, before, during, and following cyberattacks. Yet, this leadership challenge is more than simply providing rewards and, if mis-handled, can degrade trust.^[62]

Deconfliction is important, as is effective division of effort, but public-private collaboration at its best will require information sharing and task sharing without condition. Not always, but often, the US IC collaboration with international partners provides good examples. Ideally, ground-level analysts openly share experiences, even including hunches and insights. It should be likewise, with cybersecurity. Achieving this ideal will push us closer to 100 percent need-to-know transparency at each echelon of PPP organizations. The intelligence community may never allow 100 percent transparency, given the risk of compromising of sources, but to preserve trust, that should be the goal.

A joint DHS-private sector collaborative research project showcases examples of what should become our norm.^[63] The Internet Security Alliance (ISA) independently singled out two partnership programs that embodied cohesive PPP, judged as successful initiatives by private industry and government: the CSRIC Working Group 4 program; and development of the NIST Cybersecurity Framework.^[64] Best practices include: continuous interaction among key stakeholders constantly reinforced commitment to the partnership at all levels of the chain of command; and agreed-upon resourcing and collaboration in all goal-setting phases of operations.^[64] The project also highlights the importance of trust-building among federal agencies and private-sector leaders to the success of coalition forces and joint operations among our military services. Ground-level trust among employees is also essential, since many threats can and should be resolved where the rubber meets the road. After all, it was a Colonial Pipeline control room operator who discovered the ransomware attack, not the CEO.

The USG has proven capability to build reliable and robust PPP teamwork, and greater USG attention to use in cybersecurity is long overdue. The Colonial Pipeline attack caused elements of the federal government and private industry to work hand-in-hand to mobilize available resources. Enemies and attack methods are improving dramatically. We are capable of meeting the task of defending against increasingly sophisticated cyber threats, but not without prioritizing those threats and resourcing our defenses with strong leadership that recognizes and fosters the trust and collaboration needed to build a joint USG-private sector cybersecurity team.

3. Improve Vigilance Across the PPP

The world watched a ransomware attack cripple the 5,000-mile East Coast pipeline and the ensuing pandemonium at tens of thousands of gas stations. Despite USG assurances that the fuel supply would swiftly return to normal, drivers panic-purchased gasoline (some even filling large plastic bags with fuel), gas prices at some pumps reached levels not seen since 2008,^[66] then pumps ran dry at over 12,000 gas stations across the southeastern US as the panic-buying frenzy as consumers broadened their search radius for fuel. While only the first total shut-down of Colonial's gasoline pipeline system in its 57-year history,^[67] we must make it the last.

Throughout the Colonial Pipeline attack and ensuing chaos, malicious actors worldwide were learning the economic and social costs that even immature hacking groups could cause. International adversaries, both revisionist and rogue states, observed firsthand how a single cyber-attack caused panic and disruption to energy delivery in the US. To deter such criminal activity successfully, we must ensure hacking groups can no longer expect to execute ransomware extortion operations with impunity and reap multi-million dollar payoffs. Secretary of Homeland Security Alejandro Mayorkas put US ransomware losses over the past year at over \$350 million, along with a 300 percent increase in damages due to all cyber-attacks. Although the Colonial Pipeline attack was partially thwarted, more experienced hackers from well-funded revisionist regimes such as Russia or China still pose a formidable threat.

The FBI retrieved some stolen funds, but much remains to be done to avoid encore attacks. As is true of kinetic wars throughout history, defending against cyber-attacks^[68] is and must remain an unending, iterative process of incorporating new data points and assumptions. Malicious cyber-attackers will increasingly be more sophisticated, bold, and attack with greater frequency, particularly if they perceive vulnerability. Paying hackers a ransom, while perhaps not always avoidable, obviously finances yet further attacks. It also encourages copycat attacks, as does the lack of adverse, credible consequences for non-state actors and adversarial host countries alike. UK's Home Secretary Priti Patel provided many reasons why paying ransoms in the long run is bad policy,^[69] a sentiment increasingly accepted globally.

***4. Achieve More Effective Deterrence of State-Sponsored Cyber-Attacks by Clearly Defining "Red Activities," Not "Redlines."*^[70]**

As the US grapples with how best to integrate cyber operations into existing concepts of interstate war and conflict, long-accepted modalities and paradigms require fresh analysis. Colonial Pipeline exemplifies how cyber-attacks blur long-accepted conflict boundaries. While few may attribute the pipeline attack to the Russian government itself, many reports finger Russia as affording sanctuary to DarkSide, an attacker that never targets Russian-speaking assets. Whether and how the Kremlin is ever conclusively linked to this attack, such future attacks, by states, state-sponsored actors, or even by state-tolerated actors can cause devastating consequences to the US. Attribution in kinetic military operations is often^[71] sufficiently ambiguous to invite "plausible deniability." In contrast, ambiguity in cyberspace is a defining characteristic.^[72]

Ambiguity combined with the breadth of ways that cyber-domain attacks and attackers harm their victims – physically, economically, politically, socially, and/or psychologically – raise questions as to when “redlines” make sense, and if so, how they should be drawn. A better response to cyber offenses, whether by state- or non-state criminal actors, might be a well-defined array of “red activities,” each one or more of which will or simply “may” trigger serious consequences. What DarkSide perpetrated obviously would qualify as a red activity. Taking out and/or punishing DarkSide would be one response to this red activity, but what about Russia? While the public is not privy to all information at our intelligence agencies’ disposal, we do expect that Russia should want to avoid consequences for the whole spectrum of its likely involvement, whether: (a) nonfeasance; (b) the actual perpetrator, with DarkSide (or the far more formidable REvil) fronting; (c) harboring the criminal hacker, and/or knowing in advance and/or facilitating the attack; (d) having advance knowledge and failing to deter; or (e) having no advance knowledge, but doing nothing after the fact to prevent future attacks on American soil. Perhaps the spectrum of Russia’s possible complicity could be further granulated, but going forward, what is it we want to place squarely in Russia’s decision-making calculus? Russia must want to avoid being in any US crosshair, for any aspect of DarkSide’s crime, or the crimes of any other cyber crime syndicate—perpetrating, facilitating, harboring, tolerating, or even learning about it and doing nothing, after the fact. Each of these wrongs should constitute a red activity, and each should lead to a credible consequence. In their decision-making calculus, all actors should be highly motivated, if not even rewarded (or at least left alone), for proving innocence. As the lead *Washington Post* editorial on July 9, 2021, put it, “Does anyone really believe [the Kremlin] is incapable of doing anything at all about even the most prolific and prominent hackers within its borders?”^[73]

Our posture of deterrence against nuclear, chemical, biological, or other existential threats, while less flexible and far less nuanced, can provide some context. Take as examples the recent attacks by DarkSide and REvil, and Russia. Whether or not Russia was the actual perpetrator, at a minimum it clearly toed any redline we would have drawn to a pipeline or other infrastructure attack. However, culpable conduct that may attempt to shroud itself in ambiguity might well be more effectively deterred, or countered, with ambiguous but telling consequence—the where, the when, and the how we reciprocate should be on our timetable and in our decision wheelhouse. Equally important, Russia should be highly incentivized to demonstrate innocence credibly. Obviously, the best way to do that would be for Russia to “out” DarkSide and REvil, prosecute them, and/or otherwise disable their ability to victimize US interests, which Russia clearly is capable of doing. On July 13, 2021, David Sanger’s report “Russia’s most aggressive ransomware group disappeared. It’s unclear who made that happen,” confirmed that, like DarkSide, following President Biden’s warning call to Putin, REvil went dark, for one of three reasons: (a) Putin shut it down, (b) USCYBERCOM shut it down, or (c) it self-destructed.^[74]

Another challenge posed by one-shoe-fits-all redlines, which are harder to tailor to the cyber-crimes, is a fundamental difference between closed authoritarian countries and transparent

democracies. Conceptually, as President Obama learned in Syria, once drawn, a redline creates political pressure, put crudely, to satisfy bragging rights as to accountability—punishing the bad actor that crossed the line. Unlike conduct flagged as one of a list of “red activities,” the very notion of the word “redline” exposed President Obama to what’s commonly known as a “commitment trap.” Once he drew a “redline,” Syria’s subsequent transgression demanded a concrete response in order to avoid domestic, indeed, worldwide political condemnation for weakness. A free press and citizens in a democracy likely would better understand and accept ambiguity if, instead of somewhat less flexible “redlines,” we substituted a range of “red activities.”

Clearly defining one or more red activities—unacceptable behavior in cyberspace that may or may not fall short of an act of war—is critically important, and the Colonial Pipeline attack highlights a handful of such activities that should open the door to retaliatory consequence. We must work to find ways to motivate nations to want to avoid harboring or providing sanctuary to cyber-attackers. Exposing them to consequence unless they shoulder the burden of demonstrating their innocence would help achieve that. Some countries care little about their reputations (e.g., North Korea), but other countries do care (e.g., China), and the best way to establish innocence is to take visible actions to pursue, punish, and otherwise eliminate any perpetrator of harm to other nations, including its infrastructure and its citizens. The most effective way to change Russia’s decision-making calculus may be to impose an unbearably high cost if it chooses to go the wrong way, and “one size” clearly does not fit all transgressions. Rather, the response must be tailored to ramifications the offender truly cares about.

Determining how most effectively to impose costs on bad actors for implementing, or even merely tacitly approving, cyber-attacks on other nations or their citizens, would greatly benefit from the USG applying the three-layered cyber deterrence strategy urged by the 2020 Cyberspace Solarium Commission.^[75] The Commission Report goes into each of these layers, described briefly in ascending order of gravity: (a) shaping behavior; (b) denying benefits; and (c) imposing costs. Recognizing the importance of PPP, layered cyber deterrence combines and extends many traditional deterrence mechanisms in a whole-of-nation approach to cybersecurity.^[76] A facet of that first layer, deterrence by norms, includes partnering with reliable allies that are mutually motivated to define red activities and collectively impose costs on cybercriminals. The Commission also included in the first layer, for more neutral countries, deterrence by entanglement, wherein the USG creates beneficial engagements that could disappear for countries caught cyber misbehaving.

The second deterrent layer is a denial of benefits or rewards for cyberspace crimes, including intellectual property theft, malign influence operations, and significant attacks on critical infrastructure.^[77] Deterrence by denial is enhanced by reinforcing private-public sector bonds through activities such as expanding operational collaboration and pooling data on cyber-attacks.^[78] This layer impacts the adversary’s decision-making calculus by ruggedizing US

assets—making them more resilient and impenetrable—to force malicious actors to weigh the efficacy of their current resources and capabilities.

The third and most severe of the three deterrent layers imposes escalates punitive consequences for increasingly serious cyber-attacks, particularly those that threaten US national security. All deterrent layers fall under an expanded and reimagined umbrella of DoD’s “defend forward” cyber-operations doctrine. Full success will require employing these layers concurrently, continuously, and collaboratively, to include, if necessary clarity that crippling counter-cyber-attacks, and/or even use of military force are options that may become necessary at a time and place of USG choosing.^[79]

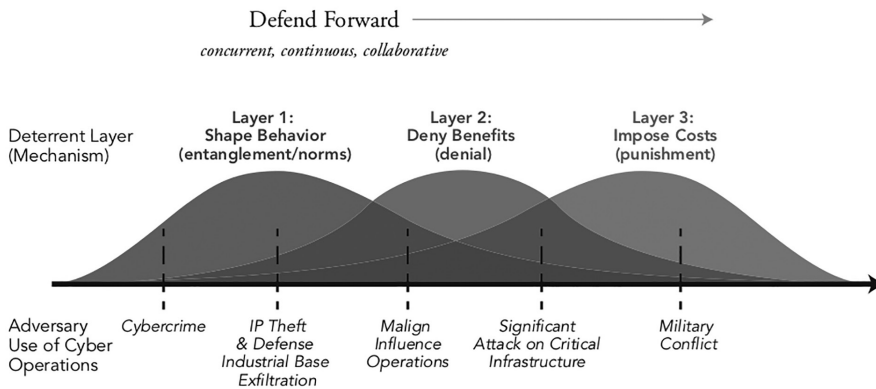


Figure 2. Layered Cyber Deterrence

These layered deterrence steps are best taken from left to right, integrating each deterrence building block, as shown in Figure 2, above.^[80] This process starts with a clear and effective cyber-defense strategy and clear national security priorities, and ends with delivering swift and decisive consequences. Again, basic cybersecurity hygiene will clear the field of most amateur hacking to allow concentrated focus on more skilled actors and critical assets. Whereas the first layer on the left in the figure above may begin with detection, more active defense moving to the right by adding attribution, increases the overall the cost in the adversary’s decision-calculus. Identifying red activities essentially works as an ocean-level berm that helps obviate the need to devote critical USG resources and energy chasing amateur hackers. It also lets near-peer adversaries know that more potent instruments of power are available, fully capable, and laser-focused on delivering punishing consequences.

5. Expand the Cybersecurity Defend Forward Doctrine

The 2018 DoD Cyber Strategy commits the US to “defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict.”^[81] This aspect of the new cyber strategy adopts the age-old adage that the best defense is a good

offense. This strategy, however, has yet to prevent increasingly bold and frequent cyber-attacks on USG agencies and businesses. For example, the Russian-based Nobelium hacking group employed the same spearfishing tactic it unleashed in the 2020 SolarWinds operation to target human rights groups critical of Putin and the U.S. Department of State (DOS), starting in January 2021 and escalating four months later in May.^[82] Ransomware tactics used against Colonial Pipeline were duplicated just weeks later in attacks on JBS and the Martha's Vineyard ferry. To those following US cybersecurity efforts, none of these attacks should be surprising. In 2019, the DHS published a report confirming critical infrastructure as an ideal target for both near-peer competitors and decentralized malicious cyber actors.^[83] Indeed, well beforehand, cybersecurity experts envisioned a scenario like the Colonial Pipeline attack.^[84]

Further efforts to formulate ransomware response strategy must more broadly define what it means to defend forward. The Biden Administration is seeking to build an international coalition to pressure those countries to hunt down and prosecute cyber-criminal syndicates they are harboring,^[85] and increasing diplomatic pressure on ransomware criminals, by pressing for change to global financial policies relating to cryptocurrency. Specifically, it seeks to establish an international standard comparable to the U.S. Treasury Department's know-your-customer requirement, to eliminate the anonymity that hides malicious actors from the law, and add anti-money-laundering mandates.^[86] Others have called for the US to deploy military and intelligence agencies in offensive cyber operations that target the technical infrastructure hackers use to employ cyber-attacks.^[87] FBI Director Christopher Wray has compared a string of high-profile ransomware attacks to national security threats posed by the September 11, 2001, terrorist attacks.^[88] Federal criminal justice and law enforcement agencies have become much more integrally involved in tackling ransomware cases. Indeed, the DOJ and FBI worked closely together, along with a ransomware law enforcement task force, to recover much of the ransom stolen from Colonial Pipeline by obtaining a warrant to seize a digital wallet containing much of the bitcoin ransom.^[89]

Ramped up US participation in PPPs will require hard, continuous private and public sector work. A well-intended Treasury Department's Office of Foreign Assets Control (OFAC) advisory in October 2020 threatened fines for "facilitating payments to criminals." This advisory was intended to deter ransom payments that would encourage more hacker demands.^[90] Even though reported ransoms paid declined in number, many viewed the OFAC advisory as unwise, because, unlike Colonial Pipeline and JBS, fewer victims would report paying ransom.^[91] Some suggest that, rather than wielding sticks, the US would benefit more by dangling carrots. John Davis, a vice president of the cybersecurity firm, Palo Alto Networks, discourages punishing victims that pay ransoms, urging instead mandatory reporting of ransom payments to federal authorities and "creating a fund to support victims who refrain from paying ransoms."^[92]

6. Create Standing Procedures in the PPP for Warp Speed Information Sharing When Key Ransomware Attacks Occur.

Colonial Pipeline deserves credit for promptly notifying federal law enforcement and government authorities of the ransomware attack. Cyber-attacks of this magnitude require an immediate communication, not an after-the-fact debrief.^[93] A key difference between a cyber battlefield and a physical battlefield is the need for response time measured in nanoseconds, not hours or even minutes. Every moment lost gives time to adversaries to cover their tracks, launder stolen funds, and/or distribute or expose stolen confidential files. Nothing beats early and ongoing USG-private sector communication and cooperation as the first post-attack step for victims struggling to minimize losses.

Knowing how the USG will use and protect information should greatly allay private corporate concerns. At least four possibilities come to mind. First, the USG may want to impose a consequence on the private entity and hold the appropriate individuals accountable for allowing a major cybersecurity incident to happen—the “gotcha” reason, either regulatory or punitive, or both. Second, the USG may want to help shut down the attack and/or interrupt a ransom payment, as occurred with Colonial Pipeline—the “help you” rationale. Third would be sharing information in an effort to inoculate others against the same or similar threat. And fourth, and strategically over the long term, would be to help the USG develop and maintain a continually updated statistical basis to craft policy. While less important for assessing blame, timeliness is especially important for the second and third potential uses of information. Corporate counsel today often blocks the proactive information sharing urged here. The USG should ensure that the private sector understands the USG is truly seeking to help and is not asking the private corporation to indict itself or its leaders for having fallen victim to a cybercrime.

Demands and penalties work, but combining those with long-term incentives likely will result in better overall response and candor from the private sector. If the USG explains why quick notice and teaming greatly benefit the company, these incentives will reinforce the trust to team success. One huge incentive will be immediate USG feedback to the victim of anything the USG has seen that may differ from the victim’s take. Private firms could be penalized for coming up short in their due diligence efforts before an attack, or for haphazardly built cybersecurity systems, but far more important is building a trusting team with buy-in from all sides. Certainly, beyond the unavoidable reputational damage already incurred, no firm should suffer for volunteering information to the USG about a ransom attack.

While not the focus of this article, technological superiority always will be key to any effective cyber defense, particularly given the sophistication of some adversary nation-states, and even other groups, like REvil. As important, however, is the human dimension, as is true whenever collaborative teaming is mission-critical. Before, during, and after an attack, attention must be paid to the ongoing human decision-making calculus, especially during the crisis. Take, for

example, the contrast between the 2013 Target and 2014 JP Morgan Chase cybersecurity data breaches. Target disclosed all known details of the cyber-attack to the public, even admitting gaps in its understanding of the attack and lack of a response plan. The press, public, and his board's backlash forced Target CEO Gregg Steinhafel to step down; Target was fined over \$18.5 million in a multi-state lawsuit, and top information officers were fired.^[94] Learning from Target's public crucifixion, when victimized by an even more serious data breach, JP Morgan Chase delayed the public announcement for many weeks while it quietly took corrective action.^[95] The takeaways here are clear: If the USG prioritizes, or even harbors as a latent goal, hunting for whoever messed up, or stabbing the already wounded, such approaches will discourage early self-reporting to the USG, and companies must also consider their reporting requirements to shareholders and the public.

The USG has taken three nascent steps toward mandating self-reporting. First, within days following the Colonial Pipeline attack, President Biden issued his May 12 Executive Order (EO) (Improving the Nation's Cybersecurity), signed, requiring all defense contractors to self-report. This step indicates clear progress, but it leaves a gaping hole— it did not include non-defense contractors. The framework for increased information sharing, outlined above in Section 2, describes what should be mandated much more broadly, to include: (a) collection and preserving data relevant to IT systems controlled by the service provider; (b) sharing such collected data; and (c) collaborating with federal cybersecurity investigations.^[96]

Second, the TSA released a May 27 directive requiring all pipeline owners and operators to (a) complete and submit cybersecurity assessments to both TSA and CISA within 30 days, (b) report all “confirmed and potential” cyber-attacks to CISA, and most uniquely, (c) appoint a 24/7-available cybersecurity coordinator to work with the USG on cyber-attack responses.^[97] Like the President's EO, however, this DHS/TSA directive applies only to a select subset of private industry (i.e., critical infrastructure service providers).

Third, Chairman Mark Warner of the Senate Select Committee on Intelligence Committee spearheaded a proposed bipartisan bill that would mandate private industry reporting a cyber incident to CISA within 24 hours.^[98] A statement by the Chairman underscores the obvious: “Voluntary sharing is no longer effective.”^[99] If enacted, this bill, anticipating private industry concerns, would exempt cyber notifications from Freedom of Information Act (FOIA) requests or use of such notifications in prosecuting service providers.^[100]

CONCLUSION

This article takes an initial cut on lessons learned following the May 6, 2021 attack on Colonial Pipeline. More information about that attack and its aftermath undoubtedly will become public over time.^[101] DarkSide sparked a national dialogue around what appears to be missing from our nation's cyber defense strategy. This article attempts to explain why recent attacks

reinforce the importance of focusing beyond the technical aspects of defense. Most essential is gathering people to work together, with strong leadership and leveraged talent, to secure against and respond to malevolent cyber activity. While the Executive Orders issued thus far are helpful as stop-gap interim measures, also essential are clear, executable legislation and inspired leadership, both for governance, and for motivation of all public and private stakeholders to meet this growing threat by embracing essential PPP collaboration that is integrated at every level of the partnership.

We have cited a clear example of one recent key cyber defense achievement in which a USG-created joint planning cell involving three relevant agencies led to demonstrable success. This example must become the rule and not the exception. We can no longer drag our feet on building an effective coalition among the nearly two dozen federal agencies now operating in cyberspace. Agency teamwork must be streamlined, and, vitally important, the USG team must partner broadly and deeply with all relevant private sector stakeholders, especially those that manage our infrastructure and that face increasingly sophisticated cyber defense threats. Required will be inspired leadership that broadens the aperture and embraces input from a very wide range of skills and personnel. Whenever America embraces its most valuable asset – the broad diversity of its citizenry and talent – it is victorious.^[102] That timeless lesson is key to our cybersecurity, just as it has been to our military, our industry, our education, and everything important we have done. However, the US and all vibrant, free market democracies, are up against adversary countries that largely have retained public ownership of critical infrastructure, and also, that exercise far more control over their private sectors than does the USG.

Leadership includes sound management of talent, but it is much more. Defeating cyber adversaries will require cohesive, tested teams that are so conspicuous that they send an unequivocal message to all would-be adversaries. Sound cybersecurity is as much about getting the roles and responsibilities of each public and private stakeholder right as it is about state-of-the-art technology. While not the focus of this article, the US enjoys an enviable, perhaps unparalleled technological edge. Maintaining that edge is an existential imperative. The focus here is more on some key lessons that, if learned, will improve the human teaming element essential to a better defense—the cyber hygiene basics, the legislative clarity, the leadership, and the public-private partnerships and PPP buy-in all essential if we are to minimize the exposure and vulnerabilities inherent in any open, democratic society like ours.

The wakeup call in the first sentence of this article underscores the missing defense so desperately needed for the US to bring its adversaries' soccer cyber scores down from a whopping 456 points to single digits. For highlighted reasons, this defense will require multiple layers of prevention, resilience, and deterrence, along with our national resolve to leverage the full range of financial, legal, diplomatic, and defense assets at our disposal as we target and respond to increasingly formidable cyber-attackers.♥

ACKNOWLEDGEMENTS

While the authors take full responsibility for any well-intended but incomplete or misguided thoughts in this article, we are deeply grateful to incoming National Cybersecurity Director Chris Inglis, a Cyberspace Solarium Commissioner, for sharing inspiration and invaluable leadership insights from which we fashioned these takeaway lessons from the Colonial Pipeline ransomware attack. West Point cadets and Naval Academy midshipmen over the years owe a great debt of thanks to this Air Force Academy graduate for the thousands of hours he has devoted, teaching them. For their editorial guidance we also give special thanks to John Costello (now with the Center for a New American Security (CNAS) and also a Cyberspace Solarium Commissioner), and formerly Deputy Assistant Secretary for Intelligence and Security at the Department of Commerce, Victoria Lee (Princeton University, 2021), Charlie Lewis (West Point, 2004), Chip Leonard & Bill Spracher (West Point, 1970), and Greenberg Traurig attorneys Paul McQuade & Scott Schipma.

NOTES

1. Dan Geer, "Cybersecurity as Realpolitik," quoting General Chris Inglis, August 6, 2014, <http://geer.tinho.net/geer.black-hat.6viii14.txt>.
2. Scott Sagan and Allen Weiner, "Would the U.S. really answer cyberattacks with nuclear weapons?" *The Washington Post*, July 11, 2021, <https://www.washingtonpost.com/outlook/2021/07/09/cyberattack-ransomware-nuclear-war/>.
3. Dustin Volz, "U.S. Blames Criminal Group in Colonial Pipeline Hack," *Wall Street Journal*, May 10, 2021, <https://www.wsj.com/articles/fbi-suspects-criminal-group-with-ties-to-eastern-europe-in-pipeline-hack-11620664720>.
4. Brian Fung and Geneva Sands, "Ransomware attackers used compromised password to access Colonial Pipeline network," *CNN*, June 4, 2021, <https://www.cnn.com/2021/06/04/politics/colonial-pipeline-ransomware-attack-password/index.html>.
5. Joseph Blount, "Testimony of Joseph Blount, President and Chief Executive Officer Colonial Pipeline Company," *Hearing Before the United States Senate Committee on Homeland Security & Governmental Affairs*, June 8, 2021, <https://www.hsgac.senate.gov/hearings/threats-to-critical-infrastructure-examining-the-colonial-pipeline-cyber-attack>.
6. Jacob Bunge, "JBS Paid \$11 Million to Resolve Ransomware Attack," *Wall Street Journal*, June 9, 2021, <https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781>.
7. Heather Kelly, "Ransom attacks are closing schools, delaying chemotherapy and derailing everyday life," *The Washington Post*, June 5, 2021, <https://www.washingtonpost.com/technology/2021/07/08/ransomware-human-impact/>.
8. Rachel Monroe, "The Go-Between: Negotiating with the hackers and the hacked," *New Yorker*, June 7, 2021, 22, <https://www.newyorker.com/magazine/2021/06/07/how-to-negotiate-with-ransomware-hackers>.
9. *Ibid.*, 23.
10. *Ibid.*; see also Lee Matthews, "2016 Saw an Insane Rise in the Number of Ransomware Attacks," *Forbes*, February 7, 2017, <https://www.forbes.com/sites/leemathews/2017/02/07/2016-saw-an-insane-rise-in-the-number-of-ransomware-attacks/?sh=3070f86a58dc>. This 2017 *Forbes* article quantified worldwide ransomware attacks in 2016 at 638 million—a 167 times increase from 2015.
11. Robin L. Fontes, Erik Korn, Doug Fletcher, Jason Hillman, Erica Mitchell, and Steven Whitham, "Jack Voltaic: Bolstering Critical Infrastructure Resilience," *The Cyber Defense Review* 5, no. 3 (Fall 2020), 45, <https://www.jstor.org/stable/10.2307/26954872>, citing Sarah Nelson, "Report: Local Gov Cyberattacks Reach Critical Level," *Government Technology*, December 18, 2019, <https://www.govtech.com/security/Report-Local-Gov-Cyberattacks-Reach-Critical-Level.html>.
12. Monroe, "The Go-Between," 23, 26.
13. Terry He, Rhoda-Mae Aronce, Lalith Dampanaboina, Justin Jose, Michael King, and Edward Cohen, 2021 *SonicWall Cyber Threat Report* (Milpitas, CA: SonicWall, Inc., 2021), 5, <https://www.sonicwall.com/2021-cyber-threat-report/#form>.
14. *Ibid.*
15. *Ibid.*, 24.
16. Nicole Perloth, *This—The Cyber-weapons Arms Race—Is How They Tell Me the World Ends*, (Bloomsbury Publishing, 2021), citing Dmitry Galov, "Remote Spring: The Rise of RDP Brute force Attacks," *Kaspersky Labs*, April 29, 2020, www.securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820. Hacking of vaccine data is further discussed in David Sanger and Nicole Perloth, "U.S. to Accuse China of Hacking Vaccine Data," *The New York Times*, May 11, 2020.
17. Ellen Nakashima, Hamza Shaban, and Rachel Lerman, "The Biden administration seeks to rally allies and the private sector against the ransomware threat," *The Washington Post*, June 4, 2021, <https://www.washingtonpost.com/business/2021/06/04/white-house-fbi-ransomware-attacks/>, accessed July 10, 2021.
18. *Ibid.*
19. *Ibid.*
20. *Ibid.*
21. Yaya Fanusie, "FinCEN's New Proposed Rule Rushes the Inevitable," *Forbes*, December 28, 2020, <https://www.forbes.com/sites/yayafanusie/2021/12/28/fincens-new-proposed-rule-rushes-the-inevitable/?sh=59b9480c4a6f>. In December 2020, FinCEN proposed new rules, such as know-your-customer (KYC) requirements on "unhosted wallets," which were not but should have been adopted.

NOTES

22. “Putin is a pro at making arrests,” *The Washington Post*, June 11, 2021. The US IC has not publicly confirmed the suspected coordination, but President Biden’s statements following the US-Russia summit underscored tension over the Colonial Pipeline ransomware attack: “I looked at him and said: ‘How would you feel if ransomware took on the pipelines from your oil fields?’” Accompanying this targeted question, the President reaffirmed the option of offensive and/or retaliatory cyber strikes as a part of the Defend Forward strategy, stating, “I pointed out to [Putin] that we have significant cyber capability. And he knows it”; see also Vladimir Soldakin and Steve Holland, “Far apart at first summit, Biden and Putin agree to steps on cybersecurity, arms control,” *Reuters*, June 16, 2021, <https://www.reuters.com/world/wide-disagreements-low-expectations-biden-putin-meet-2021-06-15/>; see also Perloth, “Cyber-weapons Arms Race,” 365, quoting Russian cybercrime expert Tom Kellermann: “There’s a pax mafiosa between the Russian regime and its cyber cartels. Russia’s cybercriminals are treated as a national asset who provide the regime free access to victims of ransomware and financial crime. And in exchange, they get untouchable status. It’s a protection racket and it works both ways.”
23. Department of Defense, *Summary: 2018 Department of Defense Cyber Strategy* (2018), 3.
24. U.S. President, “Presidential Policy Directive 41 on United States Cyber Incident Coordination of July 26, 2016,” 3, <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>.
25. While there are several reasons for this failure, the authors believe the two most important are (a) the lack of truly effective public-private partnering discussed later in this article, and (b) over-reliance by the USG on voluntary as opposed to mandatory standards. Both are essential.
26. Natasha Bertrand, Evan Perez, Zachary Cohen, Geneva Sands, and Josh Campbell, “Colonial Pipeline did pay ransom to hackers, sources now say,” *CNN*, May 13, 2021, <https://www.cnn.com/2021/05/12/politics/colonial-pipeline-ransomware-payment/index.html>. This source cites three federal officials as stating, “Among the signs that the [DarkSide] hackers were novices is the fact that they chose a high-risk target that deals in a low-margin business, meaning the attack was unlikely to yield the kind of payout experienced ransomware actors are typically looking for, the sources told CNN.” The DarkSide hackers’ apologetic response to the unintended consequence of sparking a White House investigation further indicates their amateur status.
27. United States Office of Management and Budget, “Cybersecurity Funding,” *Government Publishing Office*, March 11, 2019, 305, www.govinfo.gov/content/pkg/BUDGET-2020-PER/pdf/BUDGET-2020-PER-5-8.pdf; see also Collin Eaton and Amrith Ramkumar, “Colonial Pipeline Shutdown: Is There a Gas Shortage and When Will the Pipeline Be Fixed?” *Wall Street Journal*, May 13, 2021, <https://www.wsj.com/articles/colonial-pipeline-cyberattack-hack-11620668583>.
28. Eric Rosenbaum, “JBS cyberattack: From gas to meat, hackers are hitting the nation, and consumers, where it hurts,” *CNBC*, June 2, 2021, <https://www.cnn.com/2021/06/02/from-gas-to-burgers-hackers-hit-consumers-where-it-hurts.html>.
29. *Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack Hearing Before the United States Senate Committee on Homeland Security & Governmental Affairs*, June 8, 2021 (statement of Joseph A. Blount, CEO of Colonial Pipeline), <https://www.hsgac.senate.gov/hearings/threats-to-critical-infrastructure-examining-the-colonial-pipeline-cyber-attack>.
30. *Ibid.*
31. Kristen Eichensehr, “Public-Private Cybersecurity,” *Texas Law Review* (2017), 494.
32. This article does not flesh out how federally-sponsored Tiger Teams would benefit here, e.g., by testing, auditing, assessing critical infrastructure, and/or providing rigorous hardware and software recommendations. However, like national safety programs, if not mandated, Tiger Teams could be incentivized by amnesty periods for repairing deficiencies or otherwise curing cybersecurity vulnerabilities.
33. It is unclear as to this third cardinal cyber hygienic maxim—patching soft-ware glitches—how long in advance IT software firm Kaseya knew of its patching vulnerability before the devastating cyberattack that crippled up to 1,500 businesses. As the July 7, 2021, *The Washington Post* lead editorial explained: “The firm was aware of the vulnerability exploited [by REvil] and was working to patch it; the problem was the hackers got there first”; see also, Editorial Board, “Opinion: Biden said we’d ‘find out’ whether Putin would act on ransomware. Now we have,” *The Washington Post*, July 7, 2021, <https://www.washingtonpost.com/opinions/2021/07/07/biden-said-wed-find-out-whether-putin-would-act-ransomware-now-we-have/>.
34. Josephine Wolff, “Five myths about ransomware,” *The Washington Post*, June 10, 2021, https://www.washingtonpost.com/outlook/five-myths/five-myths-about-ransomware/2021/06/10/ble00344-c8b1-11eb-81b1-34796c7393af_story.html.
35. William Turton and Kartikay Mehrotra, “Hackers breached Colonial Pipeline using compromised password,” *Bloomberg News*, June 4, 2021, <https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password>. Mr. Blount’s testimony to the Senate Committee on Homeland Security and Governmental Affairs provides more clarity, as follows: “[W]e believe the attacker exploited a legacy virtual private network (VPN) profile that was not intended to be in use. We are still trying to determine how the attackers gained the needed credentials to exploit it... We have shut down the legacy VPN profile, and we have implemented additional layers of protection across our enterprise. It remains unclear why this profile did not require 2FA or why it still even existed.” See also *Testimony of Joseph Blount*.

NOTES

36. Many, including General Inglis during our interview, project that the vast majority of attacks would be thwarted by these three basics. While a US vulnerability gap would still exist, thwarting the vast majority of all malicious attacks would be a huge improvement over what we face today with only partial adherence to these basics.
37. Gerrit de Vynck and Rachel Lerman, “Widespread ransomware attack hits hundreds of businesses,” *The Washington Post*, July 3, 2021, <https://www.washingtonpost.com/technology/2021/07/02/kaseya-ransomware-attack/>.
38. Ibid. Before this article went to print, a broad supply-chain attack widely reported in the news on July 6, 2021, locked hundreds of small and mid-sized businesses, and tens of thousands of computers. The notorious (and highly sophisticated hacker), REvil, took credit and demanded \$70 million in ransom; see also Robert McMillan, “Ransomware Hackers Demand \$70 Million to Unlock Computers in Widespread Attack,” *Wall Street Journal*, July 5, 2021, https://www.wsj.com/articles/ransomware-hackers-demand-70-million-to-unlock-computer-in-widespread-attack-11625524076?mod=searchresults_pos4&page=1.
39. While the first of the 3 Ps in PPP typically refers to “public,” flipping the order could help underscore what we believe to be the importance, at least on many fronts, of equality of these two partners, notwithstanding the primacy of the USG in overall national security policy. Moreover, as we endeavor to explain, our legislative and executive branches of government are both essential to that. However, the backbone of success, as was true with the private sector in World War II, will be the private sector’s performance in this cybersecurity partnership.
40. Zachary Cohen, Natasha Bertrand, Kevin Liptak, and Geneva Sands, “Biden administration officials privately frustrated with Colonial Pipeline’s weak security ahead of crippling cyberattack,” *CNN*, May 11, 2021, accessed June 7, 2021, <https://www.cnn.com/2021/05/11/politics/biden-administration-ransomware-frustration/index.html>.
41. In addition to the newly created White House Office of National Cybersecurity Director, some of the many other governmental players in what is now a confusing mix of nearly two dozen agencies relevant to infrastructure attacks (many involved in the Colonial Pipeline attack) include: the FBI, Cyber Security and Infrastructure Security Agency (CISA), Department of Justice (DOJ), National Security Council (NSC), Department of Energy (DOE), Department of Homeland Security (DHS), National Cybersecurity and Communications Integration Center (NCCIC), Pipeline and Hazardous Materials Safety Administration (PHMSA), National Infrastructure Coordination Center (NICC), Federal Energy Regulatory Commission (FERC), Energy Information Administration (EIA), Critical Infrastructure Partnership Advisory Council (CIPAC), Environmental Protection Agency (EPA), National Institute of Standards and Technology (NIST).
42. In addition to the newly created White House Office of National Cybersecurity Director, some of the many other governmental players in what is now a confusing mix of nearly two dozen agencies relevant to infrastructure attacks (many involved in the Colonial Pipeline attack) include: the FBI, Cyber Security and Infrastructure Security Agency (CISA) (within Department of Homeland Security (DHS), Department of Justice (DOJ), National Security Council (NSC), Department of Energy (DOE), National Cybersecurity and Communications Integration Center (NCCIC), Pipeline and Hazardous Materials Safety Administration (PHMSA), National Infrastructure Coordination Center (NICC), Federal Energy Regulatory Commission (FERC), Energy Information Administration (EIA), Critical Infrastructure Partnership Advisory Council (CIPAC), Environmental Protection Agency (EPA), and National Institute of Standards and Technology (NIST).
43. Cohen, “Officials privately frustrated.” Although this article does not specify the number of officials and extent of their frustration, key quotes attributed to CISA definitely reveal significant frustration. CISA’s Brandon Wales softened comments saying, “We [CISA] have had historically good relationship with both Colonial, as well as the cybersecurity firms that are working on their behalf.” Yet other quotes pin down potential points of frustration: “They did not contact CISA directly...We were brought in by the FBI after they were notified about the incident... I think that there’s a benefit when CISA is brought in quickly because the information that we glean, we work to share it in a broader fashion to produce other critical infrastructure.” This quote indicates that Colonial Pipeline contacted some but not all agencies early on. For several reasons, the authors respectfully hold the USG, not Colonial Pipeline, responsible here. First, certain responsible USG authorities appear to have been timely notified. Second, it should be the USG’s responsibility, not private industries, to identify clearly those agencies that require notification, and that was anything but clear on May 6. Third, once a responsible USG official is notified, that official, not the ransomware victim, best knows which other USG agencies require notice, and that official should give that notice. Fourth, and also important, relevant USG and corporate officials alike in the midst of battle (or even after) should refrain from taking public potshots that could undermine trust or divert attention from the attacker—something CISA’s Brandon Wales appears to have recognized.
44. Carlie Porterfield, “Department of Justice Creates New Task Force to Take On Ransomware Attacks,” *Forbes*, June 3, 2021, <https://www.forbes.com/sites/carlieporterfield/2021/06/03/departement-of-justice-creates-new-task-force-to-take-on-ransomware-attacks/?sh=396e976a4b80>.

NOTES

45. Christopher Bing, Joseph Menn, and Sarah N. Lynch, “U.S. seizes \$2.3 mln in bitcoin paid to Colonial Pipeline hackers,” *Reuters*, June 7, 2021, <https://www.reuters.com/business/energy/us-announce-recovery-millions-colonial-pipeline-ransomware-attack-2021-06-07/>.
46. Ryan Gallagher and Alyza Sebenius, “JBS cyber attack raises questions about preparedness,” *Bloomberg*, June 8, 2021, <https://www.farmprogress.com/business/jbs-cyber-attack-raises-questions-about-preparedness>.
47. Larry Clinton, “Best Practices for Operating Government-Industry Partnerships in Cyber Security,” *Journal of Strategic Security* 8, no. 4 (2015), 52, DOI: <http://dx.doi.org/10.5038/1944-0472.8.4.1456>.
48. *Ibid.*, 54.
49. “A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force,” Institute for Security and Technology (April 2021), 60, <https://securityandtechnology.org/ransowaretaskforce/>.
50. *Ibid.*, 58.
51. *Ibid.*, 60 and 80, citing “Aon’s E&O | Cyber Insurance Snapshot,” <https://www.aon.com/cyber-solutions/wp-content/uploads/Aon-errors-and-omissions-cyber-insurance-snapshot.pdf>; “Cyber may never experience another soft market: Gallagher Re,” *Intelligent Insurer*, April 14, 2021, <https://www.intelligentinsurer.com/news/cyber-may-never-experience-anothersoft-market-gallagher-re-25350>; 2021 Cyber Insurance Market Conditions Report, <https://www.aig.com/us/news-andinsights/2021/jan/2021-cyber-insurance-market-report>.
52. *Ibid.*, 61 and 81, citing to Jeff Stone, “FBI turns to insurers to grasp the full reach of ransomware,” *Cyberscoop*, March 30, 2020, <https://www.cyberscoop.com/ransomware-fbi-insurance-companies-data/>; Sean Lyngaas, “Inside the FBI’s quiet ‘ransomware’ summit,” *Cyberscoop*, November 16, 2019, <https://www.cyberscoop.com/fbi-ransomware-summit/>.
53. Perloth, *The Cyber-weapons Arms Race*, 398.
54. *Ibid.*, 398-99. Norway broadly defines those companies that provide “basic national functions,” to include: financial services, electricity, health services food supply, transportation, heating, media platforms, and communications, and penalizes companies that fail to perform penetration testing, threat monitoring, and other basic security measures. In addition to strict standards for government employees, Norwegian companies have made cybersecurity training a cornerstone of their culture.
55. *Ibid.*
56. Vaughan Grant, “Critical Infrastructure Public-Private Partnerships: When Is the Responsibility for Leadership Exchanged?” *Security Challenges* 14, no. 1 (2018), <https://www.jstor.org/stable/26488490>.
57. Siobhan Gorman and Julian E. Barnes, “Iran Blamed for Cyberattacks,” *Wall Street Journal*, October 12, 2012, <https://www.wsj.com/articles/SB10000872396390444657804578052931555576700>. In 2012, the Iranians attempted to cyberattack the US in its financial heart. By one account, during a Joint Chiefs of Staff meeting following Iran’s probing cyber strikes on Wall Street, one high-profile attendee, questioning the decision requiring private corporations to cyber defend themselves, sardonically asked, if North Korea fired a missile, the US should first determine whether the missile was targeting US troops or US corporation assets before the USG would act. While the question was partly in gest, today, over a decade later, the private sector, indeed all Americans, should know the answer is clear—any attack on any part of the US will be met with swift and unequivocal response of our choosing, on our timetable, and it will be a unified, public-private coordinated response calculated not only to protect but also to punish and otherwise strongly disincentivize any encores.
58. Zachary Cohen and Geneva Sands, “Four key takeaways on the US government response to the pipeline ransomware attack,” *CNN*, May 11, 2021, <https://www.cnn.com/2021/05/11/politics/colonial-pipeline-cyber-hearing-senate-homeland-security-committee/index.html>.
59. In their research article titled “An Improvised Patchwork: Success and Failure in Cybersecurity Policy for Critical Infrastructure,” *Public Administration Review* (2020), Sean Atkins and Chappell Lawson of the Massachusetts Institute of Technology concluded, following dozens of in-depth interviews, that use of non-profit Information Sharing Analysis Centers (ISAC’s) has proven invaluable in facilitating inter-company and public-private information exchange, both within given sectors and even across different sectors. <https://www.researchgate.net/publication/346496117>. For those interested in why and how whole-of-government policymaking also requires sector-specific tailoring in order to optimize cybersecurity, Professor Lawson’s and Dr. Atkins’ superbly insightful study is a must.
60. Grant, “Critical Infrastructure Public-Private Partnerships,” 41.
61. Tasha Jhangiani and Graham Kennis, “Protecting the Critical of the Critical: What is Systemically Important Critical Infrastructure?” *Lawfare*, June 15, 2021, <https://www.lawfareblog.com/protecting-critical-critical-what-systemically-important-critical-infrastructure>.
62. *Ibid.*, 45.

NOTES

63. Internet Security Alliance, “Best Practices for Cybersecurity Public-Private Partnerships,” in *Input to the Commission on Enhancing National Cybersecurity*, 61, https://www.nist.gov/system/files/documents/2016/09/16/isa_rfi_response.pdf. This research was conducted by both the IT Sector Coordinating Council and DHS. Using a modified critical-incident method that incorporated six case studies, the joint research team developed an agreed list of a dozen best practices that embody successful PPP.
64. *Ibid.*, 62.
65. Clinton, “Best Practices,” 68. The author lists nine other best practices in this study: involve industry by using the process known as NIPP; contact stakeholders early on, ideally at the “blank page” stage; continuous and regular government-private sector stakeholder interaction; provide all stakeholders (both public and private) ample time to review and input; establish and encourage co-leadership programs; consensus partnership decision-making; communicate a genuine interest in stakeholder input; robust engagement from federal agencies in addition to DHS; government follow-through on all partnership-related decisions; and adequate, properly resourced, competent support services.
66. Will Englund and Ellen Nakashima, “Panic buying strikes Southeastern United States as shuttered pipeline resumes operations,” *The Washington Post*, May 12, 2021, <https://www.washingtonpost.com/business/2021/05/12/gas-shortage-colonial-pipeline-live-updates/>.
67. William Turton and Kartikay Mehrotra, “Hackers breached Colonial Pipeline using compromised password,” *Bloomberg News*, June 4, 2021, <https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password>.
68. Cohen and Sands, “Four key takeaways.”
69. Danny Palmer, “Ransomware: Don’t pay up, it just shows cyber criminals that attacks work, warns home secretary,” May 11, 2021, <https://www.zdnet.com/article/ransomware-dont-pay-the-ransom-it-just-encourage-cyber-criminals-that-attacks-work-warns-home-secretary/>.
70. Observations and conclusions throughout this article are those of the authors. The notion of “red activities” in lieu of “red lines” in response to cyber misbehavior was inspired by our interview of General Inglis.
71. Peter Apps, “West struggles with Russia’s ‘ambiguous warfare’ tactics,” *Reuters*, November 27, 2014, <https://www.reuters.com/article/us-russia-nato-security/west-struggles-with-russias-ambiguous-warfare-tactics-idUSKCN0JB0BU20141127>. A prominent example of Russia’s ambiguous warfare tactics that facilitated plausible deniability is the implementation of “Little Green Men,” deployed to Crimea and Eastern Ukraine in 2014. These Russian assets either wore uniforms without insignia or plainclothes.
72. The Stuxnet attack (discovered in 2010) against the Iranian nuclear centrifuges is a classic example. While there are many reports attributing this highly successful attack to some combination of the US and Israel, today, nearly twelve years later, no one knows for sure who did what. Indeed, Iranians for many months, mistaking destroyed centrifuges as normal attrition of equipment, did not even know Iran had been attacked.
73. Editorial Board, “Biden said we’d ‘find out.’”
74. David Sanger, *The New York Times*, July 13, 2021, <https://www.nytimes.com/2021/07/13/us/politics/russia-hacking-ransomware-revil.html>.
75. Senator Angus King and Representative Mike Gallagher, *United States of America Cyberspace Solarium Commission*, March 2020, 1, <https://www.solarium.gov/report>. The three ways to achieve the stated end state of reducing the probability and impact of cyber-attacks of significant consequence are (1) shape behavior, (2) deny benefits, and (3) impose costs. The first way relies on US collaboration with allies and partners, the second relies on US collaboration with the private sector, and the third relies on military cyber force projection as outlined in the defend forward strategy. Each of the three ways involves a separate deterrent layer, aiming to increase American cybersecurity by altering adversaries’ cost/benefit analysis in choosing to engage in cyber-attacks.
76. *Ibid.*, 23-24. This report explains how a layered cyber deterrence “increase(s) the costs and decrease(s) the benefits that adversaries anticipate when planning cyber-attacks against American interests.”
77. *Cyberspace Solarium Commission*, 25.
78. *Ibid.*, 24.
79. *Ibid.*, 25.
80. General Inglis created the excellent “layered cyber deterrence” chart in the text above for his service academy classrooms, which also was used for the same purpose by the Cyberspace Solarium Commission; see also *Ibid.*
81. *2018 Department of Defense Cyber Strategy*, 2.

NOTES

82. "Russia Isn't Listening," *The Washington Post*, Sunday, May 30, 2021, <http://thewashingtonpost.newspaperdirect.com/epaper/viewer.aspx>.
83. Fontes, "Jack Voltaic," 45.
84. *Ibid.*, 6.
85. *Ibid.*, 16.
86. *Ibid.*
87. Alan Suderman, "Global war on ransomware? Hurdles hinder U.S. response," *Associated Press*, June 5, 2021, <https://apnews.com/article/europe-hacking-health-coronavirus-pandemic-technology-5d69e46750abd3b40fc9adf395869c7d>. As it relates to Russia, the US could also penalize companies that provided "bullet proof" hosting services in Russia (and elsewhere) for these attackers through what is known as the IaaS executive order (currently unused). Furthermore, US companies could be barred from using Russia-based cloud service providers until Russia takes ransomware criminals more seriously; see also, U.S. President, "Executive Order 13984 of January 19, 2021, Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities," <https://www.federalregister.gov/documents/2021/01/25/2021-01714/taking-additional-steps-to-address-the-national-emergency-with-respect-to-significant-malicious>.
88. Aruna Viswanatha and Dustin Volz, "FBI Director Compares Ransomware Challenge to 9/11," *Wall Street Journal*, June 4, 2021, <https://www.wsj.com/articles/fbi-director-compares-ransomware-challenge-to-9-11-11622799003>.
89. Evan Perez, Zachary Cohen, and Alex Marquardt, "First on CNN: US recovers millions in cryptocurrency paid to Colonial Pipeline ransomware hackers," CNN, June 8, 2021, <https://www.cnn.com/2021/06/07/politics/colonial-pipeline-ransomware-recovered/index.html>.
90. Monroe, "The Go-Between," 28.
91. *Ibid.*
92. *Ibid.* The authors believe that, to ensure victimized businesses remain committed to devoting resources needed to stay ahead of cyber criminals, USG reimbursement must cover only part, not all, of the losses caused by an attack.
93. Testimony of Joseph Blount.
94. Eyder Peralta, "In Wake of Massive Data Breach, Target CEO Steps Down," *NPR*, May 5, 2014, <https://www.npr.org/sections/thetwo-way/2014/05/05/309723454/in-wake-of-massive-data-breach-target-ceo-steps-down>.
95. Emily Glazer, "J.P. Morgan's Cyber Attack: How the Bank Responded," *Wall Street Journal*, October 3, 2014, <https://www.wsj.com/articles/BL-MBB-27792>.
96. Scott A. Schipma and Paul F. McQuade, "Executive Order on Improving Nation's Cybersecurity: An Ambitious and Timely Call for a Broad Range of Cybersecurity Improvements," Greenberg Traurig, LLP, May 24, 2021, <https://www.gtlaw.com/en/insights/2021/5/executive-order-improving-us-cybersecurity-ambitious-timely-call-cybersecurity#main-content>.
97. Brad D. Williams, "DHS Cyber Order Signals Shift to 'Mandatory Measures,'" *Breaking Defense*, May 27, 2021, <https://breakingdefense.com/2021/05/dhs-cyber-order-signals-shift-to-mandatory-reporting/>.
98. Brad D. Williams, "Mandatory Cyber Reporting Within 24 Hours: Sen. Warner Bill," *Breaking Defense*, June 21, 2021, <https://breakingdefense.com/2021/06/mandatory-cyber-incident-reporting-within-24-hours-sen-warner-bill/>.
99. *Ibid.*
100. *Ibid.*
101. Thomas Brewster, "\$12 Billion Government Contractor Booz Allen Facilitates Ransomware Payments Even Though the FBI Says Never Pay," *Forbes*, June 28, 2021, <https://www.forbes.com/sites/thomasbrewster/2021/06/25/major-government-contractor-booz-allen-helps-cyber-victims-pay-ransoms--exactly-the-opposite-of-us-policy/?sh=687730984ced>. Colonial Pipeline has yet to make any comment about pertinent details discussed in this Forbes article, neither on the ransom nor on its recovery.
102. One of innumerable examples is the USG in WWII tapping private industry to build tanks; see David Vergun, "During WWII, Industries Transitioned From Peacetime to Wartime Production," *DOD News*, March 27, 2020, <https://www.defense.gov/Explore/Features/story/Article/2128446/during-wwii-industries-transitioned-from-peacetime-to-wartime-production/>. Another example was the emergency production in 1991 of engines by Detroit Diesel under Roger Penske's leadership during the Gulf War. See Joseph Siano, "AUTO RACING: The Penske Machine Is Rolling Right Along," *The New York Times*, May 31, 1994, <https://www.nytimes.com/1994/05/31/sports/auto-racing-the-penske-machine-is-rolling-right-along.html>, which recounts Penske's response to an urgent "ask" by General Norman Schwarzkopf.

THE CYBER DEFENSE REVIEW

◆ RESEARCH ARTICLES ◆

Cybered Competition, Cooperation, and Conflict in a Game of Imperfect Information

Hiram Henderson

ABSTRACT

This article proposes that “the strategy of conflict,” or game theory, can enhance joint planning processes applied to cybersecurity operations. Game theory could perhaps prove most useful during operational design for understanding actors, tendencies, and potentials actions inherent in cooperation, competition, and conflict situations. A canonical anti-coordination game, Hawk-Dove, is employed to explore equilibrium evolutionary game strategies and deterrence outcomes applicable to cyberspace operations. Tractable extensions to the Hawk-Dove game are introduced to understand mechanisms for signaling, reputation, norms, and ambiguity in deterrence. Game parameters are transferred to a model of Surprise-Attack for comparison. Advantages and disadvantages for incorporating games in the joint planning process are considered.

The Strategy of Conflict

Thomas Schelling’s *The Strategy of Conflict*^[1] is a collection of essays that presents a “vision of game theory as a unifying framework for the social sciences.”^[2] The Nobel laureate proposed calling this framework the study of “the strategy of conflict.”^[3] He regarded many conflict situations as bargaining problems with elements of opposed and common interests. For this reason, he argued the analysis of non-cooperative games was essential for understanding the theory of deterrence in international security, and more broadly for the study of “rational, conscious and artful” conflict behavior.

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



Hiram Henderson is a Senior Plans Analyst assigned to the U.S. Cyber Command (USCYBERCOM) in the J5 (Plans and Policy) directorate. His prior civilian assignment was at Joint Force Component Command-Network Warfare (JFCC-NW). As a Navy Reserve officer, he has several long-term assignments supporting information operations at the former U.S. Space Command, U.S. Strategic Command, and U.S. Special Operations Command. He studied economics at the University of Illinois, Chicago (B.S.), and University of Chicago (M.A.) and has a diploma from the Air War College. He is currently pursuing graduate study in international affairs at King's College London. He is an advocate for the wider use of games in joint planning and operational design.

In game theory, a strategy is a complete plan of actions across all possible contingencies. In a military context, a strategy is the application of military power to attain political objectives, specifically “the theory and practice of use, and the threat of use, of organized force for political purposes.”^[4] A broader definition regards strategy as “a plan of action designed in order to achieve some end; a purpose together with some system of measures for its accomplishment.”^[5]

In most of this article, strategy is used in the narrower game-theoretic sense. However, before exploring games and their application to “cybered conflict”^[6] and competition, it is helpful to review the contours of DoD cyber strategy in place, as well as mechanisms of deterrence. This will assist in ascertaining whether some game forms appear to fit stylized facts for competition or cyberspace.

Strategies in Cyberspace

The unclassified version of the *DoD Cyber Strategy 2018* prioritizes deterrence and competition in cyberspace and commits to an operating posture of “persistent engagement” and “defending forward” in cyberspace. Key passages in this regard are the following:

1) Deter malicious cyber activities: The United States seeks to use all instruments of national power to deter adversaries from conducting malicious cyberspace activity that would threaten U.S. national interests, our allies, or our partners.^[7]

2) Persistently contest malicious cyber activity in day-to-day competition: The Department will counter cyber campaigns threatening U.S. military advantage by defending forward to intercept and halt cyber threats and by strengthening the cybersecurity of systems and networks that support DoD missions.^[8]

In game logic, the *DoD Cyberspace Strategy 2018* represents a commitment to protect national security

interests in cyberspace. It is executed through defensive cyberspace operations missions as authorized in forward and/or friendly cyberspace to contest, deny and defeat malign adversary campaigns in cyberspace. In a wider sense, the strategy also serves to set conditions for deterrence and shape norms for responsible behavior in cyberspace.^[9]

Deterrence Approaches

Deterrence is the process of influencing the cost-benefit calculus of actors from taking unwanted actions. The fundamental strategies for deterrence are punishment and denial; both involve dissuasion by threats to impose costs and/or deny benefits. However, a wider view of deterrence also considers dissuasion involving reassurances or other inducements to encourage adversary restraint.^[10]

In the Age of Enlightenment, legal thinkers reasoned that it was “better to prevent crimes than to punish them” for the benefit of society. The effectiveness of deterrence by punishment was said to depend on the severity, certainty, and celerity of punishments.^[11] Such beliefs derived from utilitarian philosophy, which maintained that rational, self-interested individuals seek to maximize well-being or advantage.^[12]

Deterrence by punishment can be specific (to individuals) or general (to populations). Deterrence is absolute when an actor completely avoids a prohibited action and is restrictive when actors restrain prohibited actions to reduce the risk or severity of punishment.^[13] In the Cold War, nuclear “deterrence was specific and absolute.”^[14] However, general and restrictive forms of deterrence are the norm for crimes and political violence.^[15]

Deterrence by denial seeks to deter unwanted action by “making it infeasible or unlikely to succeed,” and by reducing an actor’s confidence of success in reaching his goals.^[16] Deterrence by denial involves commitment to the defense of vital interests.^[17]

Deterrence in cyberspace will not be absolute and lower-level malign actions can never be prevented entirely. The wide array of threat actors to include nation-states, proxies and criminal organizations, requires that deterrence in cyberspace is tailored. It can be specific or general. The Deterrence Operations Joint Concept is the framework for decisively influencing the adversary’s decision-making calculus in order to “prevent hostile actions against US vital interests.”^[18] The concept developed out of the need for a modernized deterrence framework applicable to a “broader range of adversaries and situations” in an evolving security environment^[19]

The concept frames the three primary elements of deterrence decision calculus as:

- ◆ The benefits of a course of action
- ◆ The costs of a course of action
- ◆ The consequences of restraint (of not taking the course of action we seek to deter)^[20]

Using these elements, the concept describes deterrence operations as:

Deterrence operations convince adversaries not to take actions that threaten US vital interests by means of decisive influence over their decision-making. Decisive influence is achieved by credibly threatening to deny benefits and/or impose costs while encouraging restraint by convincing the actor that restraint will result in an acceptable outcome.^[21]

Viewed through the deterrence joint concept, persistent engagement and defending forward in cyberspace can be characterized as strategies of deterrence through denial. They create frictions (or resistance costs) on malicious cyber activities from threat actors, while preserving space for diplomatic, informational, or economic responses.^[22] The game constructs used here will assume unitary actors for decision-making and will abstract from internal political-bureaucratic considerations, as well as from “audience costs,”^[23] that would otherwise affect strategy choices.

Many political economy models of war and deterrence are constructed as stage games, initially featuring periods of bargaining that transition to conflict when there is a failure to reach a diplomatic agreement.^[24] However, the canonical models used here will have elements of cooperation and conflict, and hence bargaining in a sense is built in. We also assume participation constraints are met, which means playing the game leaves actors at least as well off as from abstaining from the game.

The Hawk-Dove Game

The canonical Hawk-Dove game represents a classic model of competition and conflict in game theory. The framework was developed in biology literature to describe evolutionary strategies within a species.^[25] In this game, opponents fight over a resource, which is rival in consumption and has some value (v). Fighting for this resource involves a cost (c) that represents the damage arising from conflict.

In normal form, Hawk-Dove is a simultaneous-move game of imperfect and complete information. Imperfect information means a player is unaware of strategies other players have chosen.^[26] Complete information means that there is “common knowledge” of player types, payoffs, preferences, and strategies known by all players, and all players know that it is known by all players.^[27]

In this game, hawkish strategies broadly are non-cooperative actions involving aggression or fighting. As applied to cyberspace, non-cooperative strategies will involve the projection of power. This includes cyberspace attack—actions that create denial and/or manipulation effects, as well as forms of cyberspace exploitation, which include intelligence, maneuver, information collection, attack-specific preparations, as well as other enabling actions that prepare for future operations.^[28]

In contrast, cooperative actions will involve the absence of fighting in cyberspace, with greater emphasis on protection. This includes cyberspace security measures or actions to prevent

unauthorized access, exploitation, or damage from general threats, as well as cyberspace defense actions to defeat specific threats that have breached, or are threatening to breach, cyberspace security measures.^[29]

We consider cyberspace as a network good that grows in value as its use and connectivity expands. We will further suppose the value of cyberspace is common knowledge as is the cost of fighting. Players contest each other for advantage in this interconnected domain, competing for access, position, and control to support their informational or military objectives in the wider operational environment. This is represented in the abstract by attaining a greater share (or control) of (v).

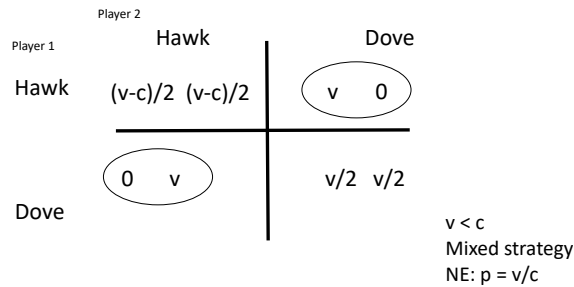


Figure 1. Hawk vs. Dove

Payoffs in the Hawk-Dove game are displayed in Figure 1 and arranged within a 2x2 matrix as follows:

$$hh \left[\frac{(v - c)}{2}, \frac{(v - c)}{2} \right]; hd [v, 0]; dh [0, v]; and dd \left[\frac{v}{2}, \frac{v}{2} \right]$$

Nash equilibrium is a core solution concept in non-zero-sum games and represents the best responses of players to the best responses of all other players.^[30] To fully enumerate equilibrium outcomes, we will consider two variants of the game with respect to the relationship of value to cost.

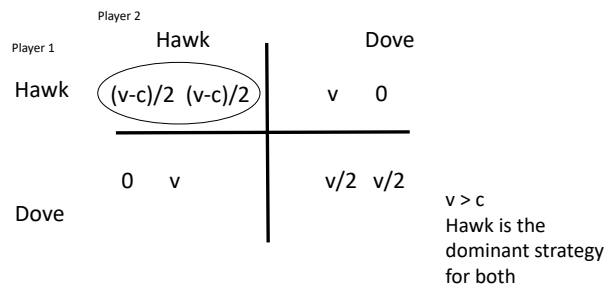


Figure 2. Prisoner's Dilemma

When $v > c$, the game reduces to a Prisoner's Dilemma in Figure 2. This variant of the game has a single Nash equilibrium, where both players find it optimal to pursue non-cooperative (Hawk) strategies in cyberspace. As long as $v > c$, an increase in cost or reduction in value will

not change the equilibrium outcome. This is because Hawk is a dominant strategy; i.e., it is the best strategy regardless of any action the other player takes. This outcome may correspond to cyberspace exploitation actions well below conflict threshold. High values along with low costs/consequences might explain why exploitation actions are so pervasive in cyberspace in equilibrium.

When $v < c$, the game becomes Chicken, and fighting becomes much more costly for the players. This variant of the game has two pure strategy Nash equilibria (where one player plays Hawk and the opponent, Dove), and one mixed strategy equilibrium, where players randomize between playing Hawk or Dove strategies. Absent prior coordination, play will not likely arrive at the pure strategy outcomes.^[31] The mixed (randomizing) strategy equilibrium is:

$$p = \frac{v}{c}$$

In equilibrium, mixing toward fighting increases with value and declines with cost.^[32] This variant of the game involves higher cost/consequence Hawk actions in cyberspace, with some scaling to a use of force. In a mixed strategy equilibrium, the frequency of fighting increases when (Hawk) actions have lower costs/consequences, and decreases when (Hawk) actions have higher costs/consequences.^[33] This may explain why lower-level cyberspace attacks are more commonplace than damaging attacks at conflict thresholds.

As players randomize, another way to see the inverse relationship between fighting and costs is in the expected value (EV) of the game, which is given by:

$$EV = \left(1 - \frac{v}{c}\right) \frac{v}{2}$$

The value of the game increases in costs because there are fewer fights.

In equilibrium, players mix to make their opponent indifferent between playing Hawk or Dove in terms of expected payoffs. Mixing is like game play in tennis, if the strategy space is limited to forehand and backhand shots. If a player becomes more proficient at her backhand, the opponent mixes in a fashion to neutralize that advantage, forcing her to play more forehand.

If there is asymmetry between players where $v > c$ for Player 1 and $v < c$ for Player 2, then fighting is more costly for Player 2. A pure strategy Nash equilibrium results where Player 1 always plays Hawk and Player 2 plays Dove. This situation involves imbalances in power and capacity. Although outside the strategy space of the game, the weaker player could find it advantageous to form alliances.

Hawk-Dove in Sequential Games

Schelling noted that a paradox arises in bargaining situations where the “power to constrain an adversary may depend on the power to bind oneself.”^[34] A player who can commit to an “irreversible sacrifice of freedom of choice” can obtain a better outcome.^[35] To win the game of

Chicken, Schelling claimed, you need to rip off your steering wheel and wave it visibly in the air for your opponent to see.

In sequential form games, moves convey information. To illustrate credible deterrence commitments in Hawk-Dove, we take game payoffs and convert them to a simple, sequential (two-stage), extended-form game of perfect information. “A game is said to have perfect information if, throughout its play, all rules, possible choices, and past history of play by any player are known to all participants.”^[36]

The extended-form game is represented in Figure 3 depicting a tree comprised of decision nodes, end nodes, and edges. A subgame begins at a decision node and includes all nodes that follow in the game tree. However, subgames cannot begin at the very first decision node of a game.

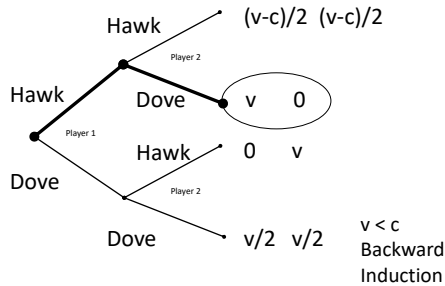


Figure 3. Hawk vs. Dove

In sequential games of complete information, the solution concept is subgame perfection. A Nash equilibrium is subgame perfect if it induces a Nash equilibrium in every subgame.^[37] Through backward induction, the subgame perfect equilibrium path of play is that Player 1 plays Hawk and Player 2 plays Dove. Here Player 1 has a first-mover advantage. However, moving first does not always confer advantage under perfect information, for example, the hand game of Rock-Paper-Scissors.

If Player 2 could irreversibly commit to play Hawk if Player 1 plays Hawk, and signal this intent, she could deter Player 1 from aggression. Player 2 may do this by reducing her options (breaking off edges) on the game tree. The subgame perfect equilibrium path becomes Dove, Dove. The off the path equilibrium, where Player 1 would play Hawk with no signal from Player 2, is not reached. See Figure 4.

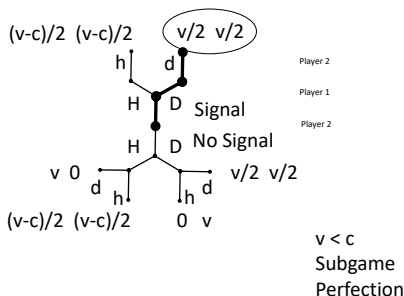


Figure 4. Hawk vs. Dove

Sequential games require trust that others play best responses, and that threats are believed. While situations involving complete and perfect information are unlikely to be encountered in cyberspace, signaling credible commitments enhances deterrence by presenting an adversary with clear choices.

Hawk-Dove with Incomplete Information

In games of incomplete information, or Bayesian games, players will not have common knowledge about other players, and may not know their types, actions, nor payoffs. Consequently, they may not believe other players’ signals.

Assume Player 1 is the uninformed player who has a probability distribution of beliefs in an information set, where (q) is the probability (belief) of encountering a commit-type Player 2, when there is a threat signal, and (r) is the probability (belief) of encountering a commit-type Player 2 without a threat signal. Assume Nature (N) makes the first move, establishing informed Player 2 types.

The commit-type Player 2 will carry out threats to retaliate if Player 1 ignores the deterrence signal. The non-commit, or normal-type Player 2 will not honor promises or threats, and always plays a best response. This situation illustrates commitment problems that often arise in game forms.^[38]

Both Player 2 types benefit from sending the same deterrence signal. The commit-type Player 2 will always send a deterrence signal, since not signaling is a dominated strategy, hence. The normal-type Player 2 also stands to gain if Player 1 is deterred, or plays Dove. Beliefs should be determined in accordance with Bayes’ Rule; however for tractability, we will consider limiting cases involving beliefs.

Suppose Player 1 does not believe the signal ($q = 0$) and acts on that belief by playing Hawk. The normal Player 2 reveals her type by playing Dove. The commit Player 2 retaliates by playing Hawk, producing a situation in which deterrence breaks down. If Player 2 types were equally encountered in nature, this would seem an unreasonable belief, and perhaps very costly where c is sufficiently high.^[39]

Alternatively, suppose Player 1 believes the signal ($q = 1$) and plays Dove. The normal Player 2 again reveals her type by playing Hawk, (see Figure 5). The commit Player 2 type plays Dove. In this case, deterrence holds.^[40] This “pooling” is an example of the “threat that leaves something to chance.”^[41]

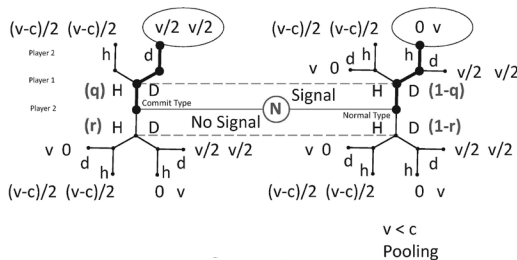


Figure 5. Hawk vs. Dove

Since Player 2's are unsure of Player 1's response, suppose Player 2's could also threaten to let things "slip out of hand." Albeit stylized, further suppose the normal Player 2 type presents Player 1 with the simultaneous-move Hawk-Dove as a continuation game, regardless of a deterrence signal.

Play in mixed strategies again yields an expected value of:

$$EV = \left(1 - \frac{v}{c}\right) \frac{v}{2}$$

which is less than

$$\frac{v}{2}$$

from the cooperative path.

In the restyled game, this enhancement has the effect of strengthening deterrence and assurances, since signaling is equilibrium and message dominated for the commit-type Player 2, and the normal-type Player 2 is now indifferent to sending a deterrence signal.

Applying the Intuitive Criterion,^[42] the commit-type Player 2 could send a signal and announce, "Seeing this signal should convince you that I am the commit Player type, since believing otherwise would not improve outcomes for other Player type, nor for yourself." If this speech is believed, Player 1 could reasonably set her belief to $(q = 1)$, resulting in a separating equilibrium, see Figure 6.

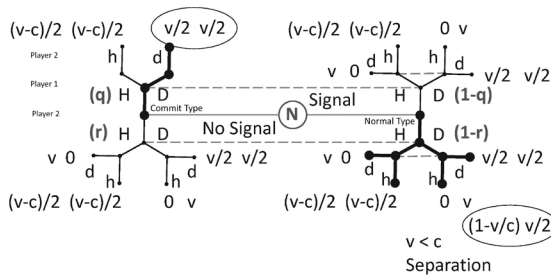


Figure 6. Hawk vs. Dove

In this restyled game, threats that leave something to chance along with credible signals can enhance deterrence in equilibrium.^[43] When player interests align, signals are more informative, and when interests diverge, signals are less informative.^[44]

In practice, decision-makers do not face black boxes as adversaries. They will have gained insights from past experiences to better understand their opponents and improve their outcomes.^[45] Knowledge isn't perfect and information asymmetries are sources of fog and friction in deterrence.^[46] If players had common knowledge of each other's beliefs, they could not agree to disagree.^[47] Errors regarding an opponent's beliefs (or intentions) explain in many cases why deterrence fails.

Hawk-Dove in an Infinite Game

Many interactions are naturally recurring. For repeated interactions, threats to eliminate future opportunities help make agreements enforceable, especially if their long-term value outweighs the gain from cheating.^[48] To explore this, we can play Hawk-Dove as a repeated stage game of imperfect information and having an infinite time horizon with a discount factor (d), where d is between 0 and 1 and represents the probability that the game continues.^[49]

The value of trying to win today through playing Hawk is balanced against rewards and punishments in the future that are discounted by d . The reward is to play the Dove strategy forever with payoffs of :

$$\left[\frac{v}{2}, \frac{v}{2}\right]$$

at each stage. However, a player can only threaten credible punishments that the other will accept, which are Nash equilibria.

Consider the Grim-Trigger strategy, where deviations from Dove are punished forever with non-cooperative (Hawk) responses. When $v < c$, which is the chicken game, the highest punishment the other is willing to accept is to play Dove with a payoff of 0, resulting in equilibrium discount factors of the following:^[50]

$$d > \frac{1}{2}$$

In equilibrium, the punished player is willing to accept an uneven distribution more than half of the time. This suggests the potential for an unstable long-run outcome. And one that could likely be renegotiated if disaffected audiences connected to this player found that distribution unacceptable.

A player could also threaten a lesser punishment by mixing forever resulting in:^[51]

$$d > \frac{c}{v+c}$$

When players are mixing, higher costs increase the equilibrium discount factor (deterrence), and there are fewer fights.

If $v > c$, which is the Prisoner's Dilemma game, the highest punishment the other would be willing to accept is to play Hawk with a payoff of:

$$\frac{(v-c)}{2}$$

resulting in equilibrium discount factors:^[52]

$$d > \frac{v}{v+c}$$

In this instance, since Hawk is a dominant strategy for both players, higher costs reduce the punishment payoff, which decreases equilibrium discount factors and lowers deterrence.

If there were payoff asymmetries between opponents ($v > c$ for Player 1 and $v < c$ for Player 2), there is no other Nash equilibrium, that Player 1 could accept as a punishment, and she could not be deterred from playing Hawk.

In infinite-horizon games, there are multiplicities of subgame perfect equilibria for sufficiently patient players. This structural problem is captured in variants of the Folk Theorem. Repeated games are also stateless games, and they would not be useful for situations where environments are changing and when strategy spaces are in transition.

Rewards and trigger punishments can induce cooperation where relationships are valued and there are patient players. However, cooperation is less sustainable when there are impatient players. A similar logic with respect to time applies to reputations and norms, since both have long-term value. When reputations are lost and norms have atrophied, both can be very costly to restore.

Comparisons to Surprise-Attack

The translation of Hawk-Dove payoffs into the simultaneous-move game of “Surprise-Attack”^[53] in matrix form appears in Figure 7 as:

$$hh [0, 0]; hd \left[\frac{v}{2}, \frac{(v-c)}{2} \right]; dh \left[\frac{(v-c)}{2}, \frac{v}{2} \right]; \text{ and } dd [v, v].$$

This game represents a model of nuclear deterrence. There are two pure strategy Nash equilibria in the upper left and lower right corners, i.e., (Hawk, Hawk) and (Dove, Dove).

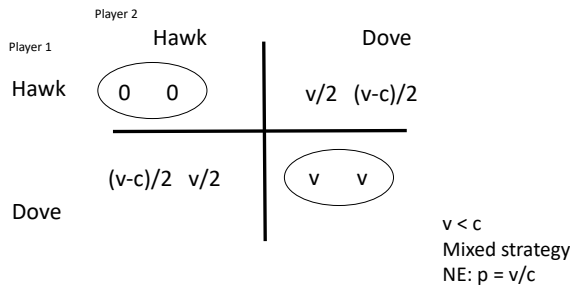


Figure 7. Hawk vs. Dove

They include what can be considered the costly outcome with payoffs $[0, 0]$, and a Pareto-dominant outcome with payoffs $[v, v]$. As before $v < c$, and in some cases, c could be considered very large. Off the equilibrium path, a player experiencing a surprise attack suffers a loss of:

$$\frac{(v - c)}{2}$$

The mixed strategy equilibrium is the following:^[54]

$$p = \frac{v}{c}$$

However, p is very low if c is considered very high. The probability that at least one player plays Hawk is very low, again if c is considered to be very high:^[55]

$$1 - \left(1 - \frac{v}{c}\right)^2$$

With imperfect information, deterrence against surprise attack appears more a matter of degree than kind in mixed strategies. However, in this game, there are strong incentives not to suffer from a surprise attack, and to respond in kind to attacks. When there is incomplete information, players will be unsure what risks the other is willing to take.^[56]

In an infinite game, where the reward payoffs are the Pareto-dominant outcome $[v, v]$, the maximum punishment the other player would accept would be $[0, 0]$. In this situation, any discount factor $[0 < d < 1]$ suffices. No matter how impatient players are, conducting a surprise attack is inefficient in the long run. The same applies to the lesser grim trigger punishment strategy of mixing.^[57]

Suppose equilibrium rewards in an infinite game are in mixed strategies. The maximum punishment the other player would accept are $[0, 0]$ payoffs. Under a grim trigger strategy, the equilibrium discount factor is the following:^[58]

$$d > \frac{v}{c}$$

which is very low, if c is very high.

In this situation, there is somewhat greater temptation for surprise attack, and trigger equilibria require less patience as costs increase. Where c is low, trigger equilibria require exceptional patience. However, where c is very high, trigger equilibria would fail only under exceptional circumstances, such as players who only lived for the present, or if fighting was a near certainty.^[59]

Reflections

While the canonical models and their extensions presented here are abstractions about competition and conflict, they fit stylized facts in connection with the pervasiveness of cyberspace exploitation, propensities for various scales of cyberspace attack as well as surprise attack. They also suggest deterrence in cyberspace is possible through “threats that leave something to chance.”

Cyberspace exploitation involves clandestine maneuvers that are generally unobserved.^[60] However, cyberspace attacks create denial effects that are eventually observed.^[61] Active

deterrence in cyberspace is thought to require attribution, credibility, and signaling,^[62] all of which underline the importance of information or intelligence in strategy.


In cyberspace, deterrence is complicated by the complexities of technical and/or political attribution to machines, tradecraft, and agency. However, for various reasons, including the growth of private cybersecurity companies, threat actors cannot presume they will enjoy complete sanctuary from attribution, and this allows for deterrence in cyberspace.^[63]

In tacit bargaining situations,^[64] where communication is impossible or incomplete, and distrust is high, norms of behavior in cyberspace may be emerging, such as agreed competition.^[65] These evolving norms are thought to be enabled by persistent engagement and defending forward, and this bears some semblance to mixed strategies in Hawk-Dove.

While inspired by evolutionary models, this analysis did not explore evolutionarily stable strategies (ESS), which are hard-wired in players. ESS are Nash equilibria that cannot be invaded or changed. In the Prisoner's Dilemma variant of Hawk-Dove, non-cooperation is the evolutionarily stable strategy. In the Chicken variant of Hawk-Dove, mixed strategies are evolutionary stable. In the Surprise- Attack game, the pure cooperative and non-cooperative strategies are evolutionarily stable.

Games contain elements of common and conflicting interests spanning the continuum of cooperation, competition, and conflict. They are bargaining situations for time or positional advantages, that do not always entail pure conflict. Games also remind us of the interdependence among relevant actors in an equilibrium. This can help planners understand the range of best responses.

Unfortunately, game theory is largely unfamiliar to planning staffs. Some models are quite complex and may not readily correspond to planning problems at hand, or could distort them.^[66] Still, some game forms might be usefully explored during operational design, where the focus is on understanding actors, tendencies, and potentials.

Games such as Stag-Hunt can help in understanding security cooperation situations. The underlying structure and strategy spaces of the Stag-Hunt coordination game mirror that of Surprise-Attack, though they involve different situations. When played against the long shadow of the future, the canonical games considered here suggest much could be gained from strengthening norms, conventions, and partnerships to deter or contain threats in cyberspace.^[67] 

DISCLAIMER

The views expressed in this work are those of the author 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. Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960).
2. Robert J. Aumann and Thomas C. Schelling, "Contributions to Game Theory: Analyses of Conflict and Cooperation," Information on the Bank of Sweden Prize Economic Sciences in Memory of Alfred Nobel (Stockholm: Royal Swedish Academy of Science, 2005), 2.
3. Thomas C. Schelling, "The Retarded Science of International Strategy," *Midwest Journal of Political Science*, 4 (2), 1960: 107-137, <https://doi.org/10.2307/2108704>.
4. The quotation was the author's description of his book. However, it also provides a succinct and classical definition of strategy. See Colin S. Gray, *Modern Strategy* (London: Oxford University Press, 1999), 1.
5. RDML J.C. Wylie, *Military Strategy: A General Theory of Power Control* (Annapolis, MD: Naval Institute Press, 2014), 14.
6. Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens, GA: University of Georgia Press, 2011).
7. Department of Defense, "Summary Department of Defense Cyber Strategy 2018" (Washington, DC: Government Printing Office, 2018), 2.
8. Ibid.
9. A case study of a norms construction through deterrence can be found in: Thomas Rid, "Deterrence Beyond the State: The Israeli Experience," *Contemporary Security Policy* 33 (1), 2012: 124-147, 2012, <https://doi.org/10.1080/13523260.2012.659593>.
10. This summarizes perspectives from Michael Mazarr in Michael J. Mazarr, "Understanding Deterrence" (Santa Monica, CA: RAND Corporation, 2018), <https://doi.org/10.7249/PE295>.
11. The seminal work on legal theory is Cesare Beccaria, "Beccaria: 'On Crimes and Punishments' and Other Writings," (original work published 1764), edited by Richard Davies (Cambridge, UK: Cambridge University Press, 1995), 103.
12. Sally S. Simpson, *Corporate Crime, Law, and Social Control* (Cambridge, UK: Cambridge University Press, 2002), 9.
13. Thomas Rid is adapting these definitions from Gibbs; see: Jack P. Gibbs, *Crime, Punishment, and Deterrence* (Amsterdam: Elsevier, 1975), 34.
14. Thomas Rid, "Deterrence Beyond the State: The Israeli Experience," *Contemporary Security Policy* 33 (1), 2012: <https://doi.org/10.1080/13523260.2012.659593>, 127.
15. Ibid.
16. Michael J. Mazzarr, "Understanding Deterrence." (Santa Monica, CA: RAND, 2018), <https://doi.org/10.7249/PE295>, 2.
17. Ibid.
18. Joint Chiefs of Staff, "Deterrence Operations Joint Operating Concept" (Washington, DC: Government Printing Office, 2006), 5.
19. Ibid., 7.
20. Ibid., 5.
21. Ibid., 8.
22. Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security* 41 (3), 2017: 44-71, <https://doi.org/10.1162/ISEC>.
23. James D. Fearon, "Domestic Political Audiences and the Escalation of International Disputes," *American Political Science Review* 88 (3), 1995: 577-592.
24. James D. Fearon, "Rationalist Explanations for War," *International Organization* 49 (3), 1995: 379-414, <https://doi.org/10.1017/S0020818300033324>.
25. John M. Smith and Geoff A Parker, "The Logic of Asymmetric Contests." *Animal Behaviour* 24 (1), 1976: 159-175. [https://doi.org/10.1016/S0003-3472\(76\)80110-8](https://doi.org/10.1016/S0003-3472(76)80110-8).
26. Robert S. Gibbons, *Game Theory for Applied Economists* (Princeton, NJ: Princeton University Press, 1992).
27. Robert J. Aumann, "Agreeing to Disagree," *The Annals of Statistics*, Vol. 4, 1976, <https://doi.org/doi:10.1214/aos/1176343654>.
28. Joint Chiefs of Staff, "Joint Publication 3-12: Cyberspace Operations" (Washington, DC: Government Printing Office, 2018).
29. Ibid.
30. John F. Nash, "Non-Cooperative Games," *Annals of Mathematics* 54 (2); 1951: 286-295. <https://doi.org/10.2307/1969529>.

NOTES

31. Robert J. Aumann and Thomas C Schelling, “Contributions to Game Theory: Analyses of Conflict and Cooperation,” Information on the Bank of Sweden Prize Economic Sciences in Memory of Alfred Nobel (Stockholm: Royal Swedish Academy of Science, 2005), 5.
32. To find the mixed strategy Nash equilibrium, a player mixes with probability (p) such that the opponent is indifferent between the two strategies. Since the game is symmetric:

$$\begin{aligned} \text{Value from playing Hawk} &= \text{Value from playing Dove} \\ p \frac{(v-c)}{2} + (1-p)v &= p \cdot 0 + (1-p) \frac{v}{2} \\ \text{which solves for} & \\ p &= \frac{v}{c} \end{aligned}$$

Substituting this value on the right-hand side gives the expected value (EV) of the game:

$$EV = \left(1 - \frac{v}{c}\right) \frac{v}{2}$$

33. The proposition is potentially testable. Taking a logarithmic transformation of mixed strategy equilibrium gives:

$$\ln(p) = \ln(v) - \ln(c)$$

which is a log-linear equation that could be estimated using suitable proxies.

34. Thomas C. Schelling, “An Essay on Bargaining,” *The American Economic Review* 46 (3), 1956: 281-306, <https://www.jstor.org/stable/1805498>.
35. Ibid.
36. Saul I. Gass, “What Is Game Theory and What Are Some of Its Applications?” *Scientific American*, June 2, 2003, 2.
37. Reinhard Selten, “Spieltheoretische Behandlung Eines Oligopolmodells Mit Nachfragertragheit – Teil I Bestimmung Des Dynamischen Preisgleichgewichts (Game-Theoretical Treatment of an Oligopoly Model with Sluggish Demand: Part I: Determination of the Dynamic Price Balance),” *Preisgleichgewichts, Zeitschrift Für Die Gesamte Staatswissenschaft Journal of Institutional and Theoretical Economics* 121 (2), 1965: 301-324.
38. Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960), 188.
39. There is no requirement for Player 1 necessarily has to hold reasonable beliefs. However, play must be consistent with beliefs. Hawk strategy is sequentially rational (i.e., optimal, given her beliefs and strategies) if:

$$\begin{aligned} \text{Value from playing Hawk} &> \text{Value from playing Dove} \\ q \frac{(v-c)}{2} + (1-q)v &> q \frac{v}{2} + (1-q) \cdot 0 \end{aligned}$$

Since $c > v > 0$, a hawk strategy is sequentially rational when the retaliation threat is not believed in the limiting case ($q = 0$) as this requires $v > 0$. The hawk strategy is not sequentially rational when the retaliation threat is believed ($q = 1$) as this requires:

$$\frac{(v-c)}{2} > \frac{v}{2}$$

which cannot happen.

40. A pooling equilibrium in messages and actions among player 2 types occurs if player 1 mostly believes retaliation threats ($q \geq .5$) and plays Dove. For the Dove strategy, sequential rationality for player 1 requires:

$$\begin{aligned} \text{Value from playing Hawk} &< \text{Value from playing Dove} \\ q \frac{(v-c)}{2} + (1-q)v &< q \frac{v}{2} + (1-q) \cdot 0 \end{aligned}$$

Since $c > v > 0$, a dove strategy is sequentially rational when the retaliation threat is believed in the limiting case ($q = 1$) as this requires

$$\frac{(v-c)}{2} < \frac{v}{2}$$

The Dove strategy is not sequentially rational when the retaliation threat is not believed ($q = 0$) as this implies

$$v < 0$$

which cannot happen.

NOTES

- 41. Thomas C. Schelling, *The Strategy of Conflict*, 187.
- 42. The Intuitive Criterion is a refinement that enables elimination of equilibria involving unreasonable beliefs for deviations off the equilibrium path, and where deviations in question would be a bad idea for a particular type. David Marc Kreps and In-Koo Cho, "Signaling Games and Stable Equilibria," *The Quarterly Journal of Economics* 102 (2), 1987: 179-221, <https://doi.org/10.2307/1885060>.
- 43. In *The Strategy of Conflict*, Schelling mainly applied "threats that leave something to chance" to incomplete information situations and sometimes to situations involving imperfect information.
- 44. Vincent P. Crawford and Joel Sobel, "Strategic Information Transmission," *Econometrica: Journal of the Econometric Society* 50 (6) 1982: 1431-1451.
- 45. Hal Brands, "The Lost Art of Long-Term Competition," *The Washington Quarterly* 41 (4), 2018: 31-51, <https://doi.org/10.1080/0163660X.2018.1556559>.
- 46. Colin S. Gray, "Maintaining Effective Deterrence," edited by Strategic Studies Institute (Carlisle, PA: U.S. Army War College, 2003), 24-25.
- 47. Aumann, "Agreeing to Disagree," *The Annals of Statistics*, Vol. 4. <https://doi.org/doi:10.1214/aos/1176343654>.
- 48. Schelling, "An Essay on Bargaining," *The American Economic Review* 46 (3), 1956: 281-306, <https://www.jstor.org/stable/1805498>.
- 49. James W. Friedman, "A Non-Cooperative Equilibrium for Supergames," *The Review of Economic Studies* 38 (1), 1971: 1, <https://doi.org/10.2307/2296617>.
- 50. The solution for an equilibrium discount factor in an infinite game uses the properties of a geometric series. For some amount (a) discounted infinitely by factor (d) giving a value of x, then x is computed by:

$$\begin{aligned}
 x &= a + ad + ad^2 + ad^3 + ad^4 + \dots \\
 xd &= ad + ad^2 + ad^3 + ad^4 + ad^5 + \dots \\
 x - xd &= a \\
 x &= \frac{a}{(1-d)}
 \end{aligned}$$

To find the equilibrium discount factor for the grim trigger strategy we set:

$$\text{Rewards Forever} > \text{Gain Today} + \text{Punishments Forever} *$$

* (Starting Tomorrow)

$$\frac{v}{2} \frac{1}{(1-d)} > v + 0 \frac{d}{(1-d)}$$

which solves for

$$d > \frac{1}{2}$$

- 51. Using the more lenient punishment, to find the equilibrium discount factor we set:

$$\text{Rewards Forever} > \text{Gain Today} + \text{Punishments Forever} *$$

* (Starting Tomorrow)

$$\frac{v}{2} \frac{1}{(1-d)} > v + \left(1 - \frac{v}{c}\right) \frac{v}{2} \frac{d}{(1-d)}$$

which solves for

$$d > \frac{c}{(c+v)}$$

- 52. To find the equilibrium discount factor for the grim trigger strategy we set:

$$\text{Rewards Forever} > \text{Gain Today} + \text{Punishments Forever} *$$

* (Starting Tomorrow)

$$\frac{v}{2} \frac{1}{(1-d)} > v + \frac{(v-c)}{2} \frac{d}{(1-d)}$$

which solves for

$$d > \frac{v}{(c+v)}$$

- 53. Schelling, "The Reciprocal Fear of Surprise Attack" (Santa Monica CA: RAND, 1958), <https://www.rand.org/pubs/papers/PI342.html>.

NOTES

54. To find the mixed strategy Nash equilibrium, a player mixes with probability (p) such that her opponent is indifferent between the two strategies. Since the game is symmetric:

$$\text{Value from playing Hawk} = \text{Value from playing Dove}$$

$$p \cdot 0 + (1 - p) \frac{v}{2} = p \frac{(v - c)}{2} + (1 - p) v$$

which solves for

$$p = \frac{v}{c}$$

Substituting this value on the right-hand side gives the expected value (EV) of the game

$$\text{EV} = \left(1 - \frac{v}{c}\right) \frac{v}{2}$$

55. The probability that both will not fire missiles is $(1 - p) (1 - p)$ or

$$\left(1 - \frac{v}{c}\right)^2$$

Consequently, the probability that at least one res missiles becomes:

$$1 - \left(1 - \frac{v}{c}\right)^2$$

56. Another nuclear deterrence game that illustrates this point is reported in:

Oliver Roeder, 2017, "How To Win A Nuclear Standoff." FiveThirtyEight, September 6, 2017, <https://fivethirtyeight.com/features/how-to-win-a-nuclear-standoff/>.

57. An allocation is Pareto optimal and efficient if there is no other distribution that can make some players better off without making others worse off.

58. To find the equilibrium discount factor for the grim trigger strategy we set:

$$\text{Rewards Forever} > \text{Gain Today} + \text{Punishments Forever} *$$

* (Starting Tomorrow)

$$\left(1 - \frac{v}{c}\right) \frac{v}{2} \frac{1}{(1 - d)} > \frac{v}{2} + 0 \frac{d}{(1 - d)}$$

which solves for

59. An allocation is Pareto dominated if another distribution exists that can make some players better off without making others worse off.

60. Joint Chiefs of Staff, "Joint Publication 3-12: Cyberspace Operations," (Washington, DC: Government Printing Office, 2018), II-7.

61. Ibid.

62. Clorinda Trujillo, "The Limits of Cyberspace Deterrence." *Joint Force Quarterly* 75 (Q4), 2014: 43-52.

63. Herbert Lin, "Attribution of Malicious Cyber Incidents." 1607. Aegis Paper Series (Palo Alto, CA: Hoover Institution, Stanford University, 2016), 43.

64. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960), 53.

65. Agreed competition amounts to "continuous strategic competition in cyberspace that does not reach the level of armed conflict." See Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation," Institute for Defense Analysis, 2019, 1.

66. Schelling, *The Strategy of Conflict*, 4.

67. Robert M. Axelrod, *The Evolution of Cooperation* (New York: Basic Books, 1984).

Technology Adoption in Unconventional Warfare

Sean W. Pascoli
Mark Grzegorzewski

ABSTRACT

As US Special Operations Command (USSOCOM) rebalances its primary focus, shifting from Violent Extremist Organizations (VEOs) to competition with Russia and China, there must be a greater emphasis on integrating cyberspace capabilities into the Unconventional Warfare (UW) doctrine. Section 1202 of the National Defense Authorization Act for Fiscal Year (FY) 2018 designates USSOCOM as the lead for irregular warfare,^[1] empowering Special Operations Forces (SOF) to leverage select irregular forces, resourced under specific legal authorities to live off the land in support of irregular warfare missions. Combatant Commands retain operational command and control despite this designation. As a recommendation on how the US should employ non-traditional forces, this article shows how nation-states like China, North Korea (DPRK), Iran, and Russia use cyber proxies to conduct combined operations. It then considers how SOF can add an asymmetric technique to unconventional warfare by using cyber-capable irregular forces at the tactical level to serve as force multipliers. Finally, the USSOCOM Resistance Operations Concept (ROC) will be expanded to demonstrate how to better engage cyber proxies within UW.

Keywords: unconventional warfare, proxies, special operations forces, Russia, China

PURPOSE

Technology adoption is more than just the employment of a particular piece of hardware, like an iPhone or a new operating system, it can also entail a new way of thinking. US Special Operations Command (USSOCOM) is in the process of strategically rebalancing and will include both Violent Extremist Organizations (VEOs) and Great Power Competition (GPC) after two decades of near-exclusive focus on counterterrorism. This strategic rebalance requires a detailed review of resources, training, and

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



Sean Pascoli, a member of the Marine Corps Forces Cyberspace Command (MARFORCYBER) Cyber Operations-Integrated Planning Element (CO-IPE) at United Special Operations Command (USSOCOM), serves as the Cyber Exercise Branch Chief in the J3-Joint Collective Training Branch. He retired after twenty-four years in the Marine Corps and transitioned into a second career as a cyber planner. A University of Chicago graduate (1990) with a BA in Political Science and two master's degrees from the University of South Florida (USF) in Cyber Intelligence and Cybercrime, Mr. Pascoli also holds graduate certificates from USF in Information Assurance and Digital Forensics. His area of academic focus is the nation-state use of cyber surrogates and proxies.

doctrine as a result of the national security paradigm returning to nation-states and deterring near-peer adversaries. As a result, the US Government (USG) now employs the full-spectrum of information operations to compete in the gray space between peace and armed conflict. To adapt and compete, USSOCOM must become more versatile and resourceful in applying limited assets and resources to this fight. Pointing to the need to adapt, the Theater Special Operations Command Manning Review found that a core USSOCOM mission that should be re-invigorated and implemented in several Geographic Combatant Command Campaign plans is Unconventional Warfare (UW).^[2]

The Joint Staff defines UW as “activities conducted to enable a resistance movement or insurgency to coerce, disrupt or overthrow a government or occupying power by operating through or with an underground, auxiliary and guerrilla force in a denied area.”^[3] A critical, detailed USSOCOM planning document for applying UW is the Resistance Operating Concept, which is a reflection on the past in that it addresses the need for countries to resist against occupation, just as Eastern Europe did during the Cold War.

This new breed of Russian threat, hybrid and unconventional, violent and non-violent, has forced USSOCOM to look for a different approach in this space since the doctrines of combined arms maneuver, counterterrorism, and counterinsurgency may no longer apply.^[4] The Kremlin's view of warfare views the human mind as the key terrain which means the next war will be won in the information domain by psychological warfare.^[5] To win here, Russia will deploy its less robust conventional forces only when absolutely necessary.^[6] Instead, Russia will focus its resources by forcing its adversary's military and citizens to respond to the attacker and expend its own resources.^[7] In response, USSOCOM's answer to this “new” Russian way of war is the Resistance Operations Concept (ROC); a new interpretation of the centuries-old theory of UW.^[8]



Dr. Mark Grzegorzewski, a Resident Senior Fellow at Joint Special Operations University (JSOU) currently focused on researching cyberspace operations and artificial intelligence (AI). He is recently published in *Special Operations Journal* on “Demystifying Artificial Intelligence through DoD Education” and also “Supporting Resistance Movements in Cyberspace.” He also has a chapter in an edited volume titled “Russian Cyber Operations: The Relationship Between The State And Cyber Criminals.” He created JSOU’s *Quick Look* series with a publication on AI, and a forthcoming *Quick Look* piece on Cryptocurrency. Dr. Grzegorzewski holds a Ph.D., M.A., and B.A. in Political Science from the University of South Florida, along with a graduate certificate in Globalization Studies.

ROC Needs More “Cyber”

The Resistance Operating Concept was established to support the Eastern European members of the North Atlantic Treaty Organization (NATO): Estonia, Latvia, and Lithuania. These countries are attempting to withstand Russia’s increasing aggression to reclaim its former territories: it uses various methods of hybrid warfare, combined with its advantage of interior lines to quickly seize the Baltic countries. These three countries are vulnerable as they are part of the former Soviet Union. Short of the ability to resist, these Eastern European states are threatened by Russia’s operational dexterity and the lack of a large Europe-based US conventional force to credibly deter aggression.^[9] As Estonia, Latvia, and Lithuania lack a readily available counter to Russia’s aggression, the Resistance Operating Concept supports them by addressing the inadequacies of the conventional military, national defense planning and preparation by supporting a Total Defense model where the citizenry is the primary actor instead of the government.^[10] Of relevance for SOF to consider, perhaps given that the citizen is at the center of this model where they must always be prepared for invasion, the Resistance Operating Concept perhaps should be known as the Persistence Operating Concept.

Total Defense is ideally suited for countries who share a border with hegemonic powers, and “includes all the necessary activities to prepare a nation for conflict in defense of its independence, sovereignty, and territorial integrity; and consists of both civil and military defense.”^[11] It encompasses all societal functions needed to mobilize the support necessary to defend the nation and its territorial integrity against armed attack.^[12] USSOCOM’s support to Baltic resistance would primarily consist of Special Forces Operational Detachment-Alpha, or A-Teams,^[13] executing UW campaigns by employing proxies to enable the resistance in a contested area.

But the current ROC, insofar as deployable UW cyberspace tools, is virtually non-existent in SOF A-Teams, due to several reasons ranging from capabilities to capacity, as well as risk aversion and ignorance of authorities. Currently, A-Teams are insufficiently prepared to conduct cyber operations. To task an A-team with such a mission would be a significant leap forward, but would also be very dangerous. Yet, far too often authorities are cited to excuse inaction in cyberspace. The 2018 National Cyber Strategy,^[14] the 2018 National Defense Authorization Act (NDAA), and the 2021 NDAA Section 1299, Functional Center for Security Studies in Irregular Warfare)^[15] all point to a maturation of public cyber policy relating to SOF forces. This flood of newly published unclassified national-level strategy and policy documents empowers SOF to act within its mission set.

This deficiency can be mitigated by taking a page out of Russia and China's playbooks and employing cyber proxies that can effectively impose costs on the adversary.^[16] Cyber proxies serve as intermediaries that conduct or directly contribute to an offensive cyberspace action that is either actively or passively enabled by a beneficiary.^[17] Fiscal authority exists to leverage select foreign forces in support of irregular SOF warfare missions, and cyber forces can be employed by A-Team forces.

Cyber Proxies and SOF

One DoD concern may be that cyber-capable irregular forces can employ unsanctioned cyber operations that pose an unacceptable risk for senior leaders. Nothing prevents the use of kinetic capabilities that cause serious physical damage, but some DoD senior leaders still see cyberspace operations as a bridge too far in UW campaigns. The DoD must overcome this unfounded fear that cyberspace operations should be reserved for existential, strategic threats against the US so that these capabilities can be normalized in all DoD operations that have signed Execute Orders. Many nations, including the US' biggest adversaries—China, Russia, Iran, and North Korea—have normalized the use of cyber proxies with great success.^[18] As such, SOF should be wargaming these new tradecraft methods and techniques to prepare our Forces to conduct combined operations against our adversaries in the multiple domains where they now confront us.

Including cyber-capable irregular forces as integral to SOF principles of support to UW is not an intellectually heavy lift and has the second- and third-order effects of protecting the US from its adversary's ability to conduct cyber-attacks by causing them to focus inward on domestic security, and lose trust in their cyber proxies, thereby allowing the US to maintain its technological edge in the cyber domain.^[19] The effectiveness of an insurgency is well known to the DoD, especially SOF, which for over two decades has fought to overcome various insurgencies in Afghanistan and Iraq—insurgencies that massively drained US human and financial resources. Embedding a cyber component or line of operation within the ROC would result in the cyber proxy serving as a force multiplier in any UW campaign. For example, supporting cyberspace UW/ROC by enabling infrastructure and networks, used by

hacktivists and other wired individuals in an occupied Baltic country, would force Russia to look inward and drain its capabilities and capacity to fight a digitally enabled insurgency. By enabling infrastructure and networks, they could be used for either commercial or military purposes so only the intention of use changes, not the infrastructure. Such distractions would erode the adversary's ability to conduct external cyberspace operations or otherwise attack American targets. A cyber-enabled UW campaign in Eastern European countries would enable SOF cyber proxies to enhance the overall UW/ROC campaign plan.

It's High Time to Implement Cyber UW

Cyber-enabled UW is not a new concept. Among the Special Forces practitioners who have published on the topic, the foremost advocate has been COL(Ret.) Patrick Duggan. He was the first to propose sending UW pilot teams into cyberspace.^[20] Duggan envisioned these teams as influencing the environment by targeting social media networks, deploying UW pilot teams that essentially lived off the land by employing dual-use commercial technologies, indigenous equipment, and local networks of influence. Once the environmental conditions were established locally, these UW pilot teams could influence social media's gray and dark networks from their home base. Duggan correctly notes the ability of UW pilot teams is constrained only by their authorities. This remains a hurdle, even though some authorization has in recent years been pushed down to the operational levels, as some Commanders remain reticent to delegate as advocated by Duggan, given the unintended operational effects that sometimes materialize with social media operations.

Duggan also urges the use of cyberspace capabilities to be employed in Special Warfare (foreign internal defense, UW, and counterinsurgency).^[21] Special Forces (SF) in Duggan's view could exploit cyberspace to identify, assess, and evaluate resistance leaders and capabilities, and otherwise better understand the environment in which they are operating. Once armed with the proper infrastructure and an operational mission, these Cyber UW pilot teams could also deploy to the physical environment and further nurture relations with resistance forces.

Duggan persists in arguing for man-machine teaming in UW, urging the DoD to keep pace with its competitors and increase the use of emerging technology, including 3-D printing during operations.^[22] He also promotes cyber-enabled UW financial warfare, using cyberspace to distort the price of goods, and SOF's ability to compromise the confidentiality, integrity, and availability of open adversary networks using cyber tools. One challenge Duggan briefly addresses without elaboration is the potential effect of man-machine teaming micromanaging tactical actions from operational level commands in the same way that the telegram was used to micromanage during World War I. This remains a valid concern today and requires continued attention to balance between a Commander's need to know with operational flexibility.

Duggan also argues the DoD must recognize that the character of conflict is changing, and SOF is perfectly suited to operate in cyberspace given that cyber-warfare is essentially human-warfare and SOF specializes in the human domain.^[23] Employing SOF's light footprint and unconventional mindset in the cyber domain provides the DoD with another tool in its deterrence strategy. As such, SOF must continue to understand an adversary's environment, including factors that drive its behavior and each society's relationship with information. SOF can then exploit these insights and thereby divert the adversary inward.

Agreeing with Duggan's arguments, Benjamin Brown in 2018 called for the creation of a "CYBERSOC" (Cyber Special Operations Command), nested within USSOCOM, arguing the need for cyber operators to support special operations.^[24] Thus, CYBERSOC would support the twelve special operations core activities and conduct its own missions with cyber as the primary line of effort. Brown and Duggan agree that cyberspace overlaps with the human domain, making SOF ideally suited to take on the cyberspace special operations mission set.

COL (Ret.) Brian Petit, another former US Army Special Forces practitioner, envisions a role for SOF in cyberspace via social media.^[25] He sees social media and the way it can enable unconventional warfare an essential part of any UW campaign. The social media environment reflects reality in some ways and SOF can use this space to identify resistance potential and could conceivably support a resistance movement. This could include amplification of social media messages, providing communications equipment, creating social media accounts, and even influencing messaging. To Petit, SOF's role in social media should always be set to "on," whether gathering targeting data or shaping/suppressing information.

This discussion contributes to UW cyber literature by explaining how a new actor, cyber-capable irregular forces, could work with UW forces, and builds upon the ideas from the Resistance Operating Concept. Concepts of resistance movements and unconventional forces are imperfect fits, and only one of many types of social movement that unconventional warfare supports and leverages. Yet the insertion of more cyberspace capabilities into UW writ large will give SOF greater impact in navigating revolutionary and insurgent social movements.

Cyber-Capable Irregular Forces

As Russia seeks to gain influence in cyberspace, the DoD has been directed to engage in cyberspace more robustly below the level of armed conflict. Cyber proxies mitigate attribution concerns and allow DoD to execute offensive cyberspace operations. For some time now, Russia, China, Iran, and North Korea have conducted joint operations with cybercriminal elements that mask their nation-state activities, and countering these activities in-kind it would be a force multiplier for UW campaigns.^{[26],[27]}

Their label as criminals of course poses challenges for DoD to leverage cybercriminals to counter enemy behavior, without attribution. That said, the definition of crime varies widely

in different countries. For example, individuals pushing back against a corrupt regime or exposing wrongdoing could be labeled as criminals. Therefore, working with these cyber-capable irregular forces would serve as an agile, responsive UW force that could effectively degrade threat actions below the level of armed conflict. By identifying, assessing, and evaluating these forces during the preparation phase, SOF-enabled infrastructure and networks in a UW cyberspace campaign could help counter Russian aggression in Eastern Europe.

Where Should Cyber Fit?

The seven phases of SOF support to UW (see Figure below) serve as an intellectual framework for UW cyber activities and operations and are easily adaptable to the cyber domain and a cyber-enabled ROC.^[28] These phases will not always run sequentially. Indeed, operators will move in all directions among the UW phases and sometimes even operate multiple phases simultaneously.

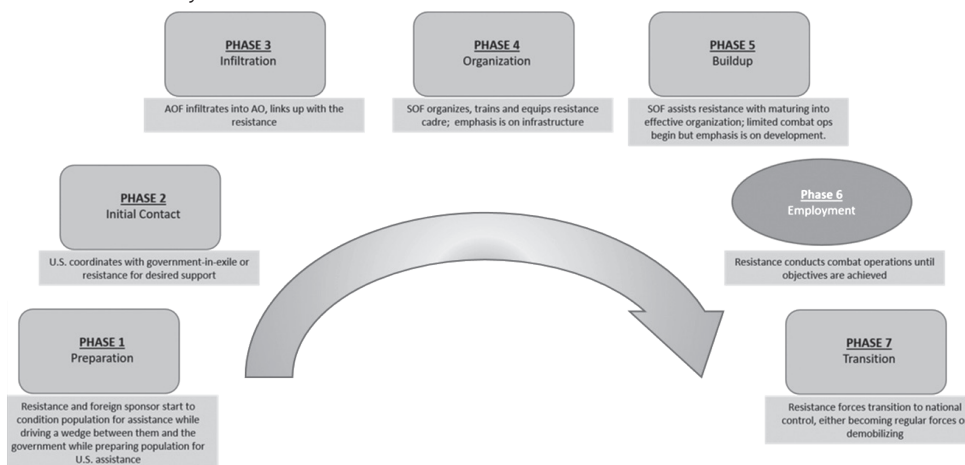


Figure 1. Seven Phases of Unconventional Warfare

1. Phase I Preparation

- a. **Physical Domain:** Resistance and external sponsors conduct psychological preparation to unify the population against the occupier and prepare the population to accept US support.
- b. **Cyber Domain:** Analyze online information environments; ask how the society influences and responds to social media; identify online opposition groups in target countries. Include hacktivists, peacefully opposed organizations, university computer clubs, and cybercriminals. Examine the online environment; identify risks to mission and threats to the occupying force (including leverageable dissidents within the occupying force). Determine (a) cyber-capable irregular force access to occupier's open networks, and (b) available open-source and living-off-the-land tools^[29] for resistance force to leverage against the occupier.

2. Phase II Initial Contact

- a. **Physical Domain:** US agencies coordinate with allied governments-in-exile or resistance leaders for needed US support.
- b. **Cyber Domain:** Establish contact with hacktivist leaders and online elements through forums and chatrooms; demonstrate technical ability to support cause. Use clandestine methods and applications (i.e., virtual private network (VPN), the onion router (TOR), disposable e-mail accounts, etc.) to reach cyber-proficient opposition. Use overt methods and applications to reconnoiter networks connected to the Internet of Things.^[30]

3. Phase III: Infiltration

- a. **Physical Domain:** SOF infiltrates into the operational area, establishes communications with its base, and contacts resistance organization.
- b. **Cyber Domain:** Phase II and III combine in the cyber domain since infiltration can be digital until trust is developed to enable contact in the physical domain. Infiltration is also an infrastructure-specific effort that maintains traffic anonymity into the area of operations and contacting hacktivist leadership. This phase may also include the introduction and coordination of the cyber proxy and the physical proxy, (if not one and the same). SOF and cyber-capable irregular force communication can be conducted via ad hoc wireless, meshed networks.^[31]

4. Phase IV: Organization

- a. **Physical Domain:** SOF organizes, trains, and equips resistance cadre with an emphasis on developing infrastructure.
- b. **Cyber Domain:** Provide communication methods or forums for hacktivists to conduct Command & Control (C2) and receive guidance, capabilities, and training from SOF cyber, potentially including Force Protection (ForcePro) and use of open-source intelligence (OSINT) for targeting. SOF can transfer money to the cyber-capable irregular forces via an obscured ledger cryptocurrency that conceals the sponsor. SOF can also provide various 3-D printable designs that the cyber-capable irregular forces could employ and identify dual-use technologies.

5. Phase V: Buildup

- a. **Physical Domain:** SOF assists cadre expansion into an effective resistance organization; while emphasis is development, limited combat operations may be conducted.
- b. **Cyber Domain:** Provide offensive cyber capabilities training and limited system and target information to increase capability and capacity to achieve desired outcomes. Have proxy forces find open-source code, as well as code and tools from dark-net hacker marketplaces, for cyber-capable irregular force use. Work with cyber-capable irregular

forces to produce both cyber effects and real-world effects. Create coordinated domain crossing effects for maximum effect.

6. Phase VI: Employment

- a. **Physical Domain:** UW forces conduct combat operations until linkup with conventional forces or end of hostilities.
- b. **Cyber Domain:** Hacktivists conduct offensive cyber operations until strategic goals below the level of armed conflict are achieved, or until the desired decrease in the target nation's external cyber operations is reduced to acceptable levels. These effects should be scalable and reversible. Observe cyber-capable irregular forces to prevent employing effects that could harm critical infrastructure or the private sector that could also harm the occupied population. Also, ensure that cyber-capable irregular forces' effects are not undermining government-in-exile's political objectives. Finally, cyber-capable irregular forces may display hacked or other compromising, occupying force information to influence the information domain.^[32]

7. Phase VII: Transition

- a. **Physical Domain:** UW forces revert to national control, shifting to regular forces or demobilizing.
- b. **Cyber Domain:** The cyber proxy demobilizes and promotes national stability, ensuring the free information flow on the internet. Cyber-capable irregular forces restore cyber effects to the national government, retaining connectivity to infrastructure and networks. Preserve plausible deniability as to DoD affiliation, thereby (a) giving cyber-capable irregular forces and host nation government legitimacy with the population for home grown cyber operations, and (b) allowing the sponsoring government to employ similar tactics, techniques, and procedures elsewhere.

CONCLUSION

What is old is new again. UW, which had assumed a tertiary role in the US' counterterrorism fight, has returned with a vengeance. As the threat of Russian dominance hangs over Eastern European countries, resistance within the context of unconventional warfare has once again become relevant. Instead of blindly following lessons of the past, the US must use technology and cyberspace within UW to effectively combat today's threats. The new thinking we advocate includes employing cyber-capable irregular forces in the cyber domain by enabling infrastructure and networks against occupying forces. What matters when enabling infrastructure and networks is intentions, and how it is engaged. Thus, SOF must persist in this space 24/7. Non-cyber resistance forces are routinely armed with lethal weaponry. DoD's reluctance to engage cyber proxies must come to an end.

Until senior leaders' comfort level with cyberspace operations matches their comfort level with tactical nuclear weapons, amphibious assaults, and carpet bombing, US military forces will continue to operate with one hand tied behind their back. The US must increase efforts at developing, enabling, and maintaining infrastructure and networks to take full advantage of its Cyber Mission Teams and Cyber Operating Forces. Once this paradigm shifts and US-SOCOM embraces the centrality of enabled infrastructure and networks, SOF will be much better positioned to compete more effectively with adversaries in the cyberspace domain, and, indeed, across domains. Until then, its technological edge in military cyberspace over near-peer competitors will continue to erode.♥

NOTES

1. Deputy Secretary of Defense, “Directive-type Memorandum (DTM)-18-005 - Authority for Support of Special Operations for Irregular Warfare (IW),” August 3, 2018, <https://fas.org/irp/doddir/dod/dtm-18-005.pdf>.
2. Hal Brands and Tim Nichols, “Special Operations Forces and Great-Power Competition in the 21st Century,” American Enterprise Institute, August 2020, <https://www.aei.org/wp-content/uploads/2020/08/Special-Operations-Forces-and-Great-Power-Competition-in-the-21st-Century.pdf>.
3. Kevin Stringer and Glennis Napier, *Resistance Views: Essays on Unconventional Warfare and Small State Resistance*, Tartu Resistance Seminar (Tampa: JSOU Press, 2019), 66.
4. Nicu Popescu and Stanislav Secieru, eds., *Hacks, Leaks and Disruption-Russian Cyber Strategies* (Paris: European Union, Institute for Security Studies, 2018).
5. Booz Allen Hamilton, *The Logic Behind Russian Military Cyber Operations* (Washington, DC: Booz Allen Hamilton, 2020).
6. Quentin Hodgson, Logan Ma, Krystyna Marcinek, and Karen Schwindt, *Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace*, (Santa Monica, CA: RAND, 2019).
7. Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020).
8. Otto Fiala, *Resistance Operating Concept* (Tampa: JSOU Press, 2019).
9. Kevin Stringer and Glennis Napier, *Resistance Views: Essays on Unconventional Warfare and Small State Resistance*, Tartu Resistance Seminar (Tampa: JSOU Press, 2019).
10. Otto Fiala, *Resistance Operating Concept* (Tampa: JSOU Press, 2019).
11. Ibid.
12. Kevin Stringer and Glennis Napier, *Resistance Views: Essays on Unconventional Warfare and Small State Resistance*, Tartu Resistance Seminar (Tampa: JSOU Press, 2019).
13. There are six A detachments in each Special Forces company. A major or a senior captain leads the 12-man team. Second in command is a warrant officer. Two noncommissioned officers, or NCOs, are trained in each of the five SF functional areas: weapons, engineering and demolitions, medicine, communications, operations and intelligence, and comprise the remainder of the team. All team members are Special Forces qualified and cross-trained in different skills as well as being multilingual.
14. White House, “National Cyber Strategy,” September 2018, <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.
15. 116th Congress, “SEC. 1299L. Functional Center for Security Studies in Irregular Warfare,” *Small Wars Journal*, December 30, 2020, <https://smallwarsjournal.com/blog/sec-1299l-functional-center-security-studies-irregular-warfare>.
16. Tim Maurer, *Cyber Mercenaries* (Cambridge, UK: Cambridge University Press, 2018)
17. Ibid.
18. Quentin Hodgson, Logan Ma, Krystyna Marcinek, and Karen Schwindt, *Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace* (Santa Monica, CA: RAND, 2019).
19. Tim Maurer, *Cyber Mercenaries* (Cambridge, UK: Cambridge University Press, 2018).
20. Patrick Duggan, “UW in Cyberspace,” *Special Warfare* 27, no. 1 (2014): 68-70.
21. Patrick Duggan, “Strategic Development of Special Warfare in Cyberspace,” *Joint Force Quarterly*, October 1, 2015, <https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-79/Article/621123/strategic-development-of-special-warfare-in-cyberspace/>.
22. Patrick Duggan, Man, Computer, and Special Warfare, *Small Wars Journal*, January 4, 2016, <https://smallwarsjournal.com/jrnl/art/man-computer-and-special-warfare>.
23. Patrick Duggan, Why Special Operations Forces in US Cyber-Warfare? *The Cyber Defense Review* 1, no. 2 (2016), 73-79.
24. Benjamin Brown, “Expanding the menu: The case for cybersoc,” *Small Wars Journal*, January 5, 2018, <https://smallwarsjournal.com/jrnl/art/expanding-menu-case-cybersoc#:~:text=The%20United%20States%20military%20should,U.S.%20interests%20and%20national%20security>.
25. Brian Petit, Social Media and UW, *Special Warfare* 25, no. 2 (2012): 20-28.
26. Jonathan Lusthaus, *Industry of anonymity: Inside the business of cybercrime* (Cambridge, MA: Harvard University Press, 2018).
27. Mark Grzegorzewski, “Russian Cyber Operations: The Relationship between the State and Cybercriminals” in *Historical and legal aspects of cyber attacks on critical infrastructure*, edited by Denis Čaleta and James F. Powers (Ministry of Defense, Republic of Slovenia, Joint Special Operations University, and Institute for Corporate Security Studies, Ljubljana, Slovenia, 2020), 53-64.

NOTES

28. Kevin Stringer and Glennis Napier, *Resistance Views: Essays on Unconventional Warfare and Small State Resistance*, Tartu Resistance Seminar (Tampa: JSOU Press, 2019).
29. Living-off-the-land tools include those instruments that are low signature, low attribution, and low power.
30. David Kilcullen, "The Evolution of Unconventional Warfare," *Scandinavian Journal of Military Studies* 2, no. 1 (2019).
31. Patrick Duggan, "To Organize Cyber, Humanize the Design," *Small Wars Journal*, November 21, 2016, <https://smallwars-journal.com/jrnl/art/to-operationalize-cyber-humanize-the-design>.
32. Megan K. McBride, Zack Gold, and Kasey Stricklin, "Social Media Bots: Implications for Special Operations Forces," Center for Naval Analysis, September 2020, https://www.cna.org/CNA_files/PDF/DRM-2020-U-028199-Final.pdf.

RT and the Element of Disguise: Russia's Information Weapon

Tobias Redington

ABSTRACT

Western journalists have labelled RT, Russia's state-controlled international television network, as the Kremlin's "lie machine," "Putin's weapon of mass deception," or even as an active participant in "Russia's propaganda Blitzkrieg".^[1] However, there is less scholarship on the network, particularly addressing the reasons for its reported success at recruiting a global audience.^[2] After a brief topography of Russian foreign-language broadcasting, this article explores this gap in three stages, first explaining why disguise is important to RT's role as Russia's information weapon. During moments deemed critical, using the poisoning of Sergei and Yulia Skripal in 2018 as a case study, RT flooded the information space with false or misleading narratives to disrupt Western broadcasting. Here, critical moments denote instances of heightened tension between Russia and the West. This is a subversive campaign that utilizes information within the framework of Giles and Kelushov. During non-critical periods, RT imitates Western news outlets in content and cosmetics to build an image of authenticity and attract a trusting audience. This, in turn, amplifies RT's subversive campaign during critical moments. Interviews between RT editor-in-chief Margarita Simonyan and Russian journalists support my analysis of RT as Russia's information weapon and provide a historical perspective on the importance of disguise since the 2008 Georgian War. Second, the article explores RT's engagement to demonstrate that this tactic is effective in attracting a faithful audience and, therefore, disrupting the narrative space. Finally, the article discusses the possibility of Western countries removing RT's broadcasting licence, and analyzes disputes between the UK's broadcasting regulator, Ofcom, and RT.

© 2021 Tobias Redington



Tobias Redington, is an alumnus of the Cambridge Security Initiative's 2019 International Security & Intelligence Programme, focuses on psychological operations and disinformation campaigns. He holds an MA in Intelligence & International Security from King's College London and a BA in Classics from the University of Exeter, UK. Tobias has also conducted research into ISIS recruitment magazines at Universität Mannheim, Germany.

Russia's Information Weapon

Founded in 2005 as “Russia Today,” purportedly to provide “a Russian viewpoint on major global events,” the state-funded broadcaster has developed a global brand.^[3] RT's owner is an ANO, “Autonomous Non-Commercial Organisation,” or non-profit, called TV-Novosti. A rebrand of the organization took place in 2009, which formally dropped ‘Russia’ from its name, though the organization is commonly known by its original name. Editor-in-chief Margarita Simonyan claimed that this rebrand took place “so as not to scare the audience” by detaching the outlet from its Russian roots before going global and delivering content in English, Spanish, French, German, and Arabic.^{[4],[5]} Sputnik is another state-funded media outlet with close links to RT, such as sharing Simonyan as editor-in-chief and sharing a common editorial stance. Hinting at organizational confusion, RT hosts its weekly show called Sputnik. Moreover, *Sputnik* itself is owned by Rossiya Segodnya, which translates to “Russia Today.” However, RT remains Russia's most well-known and wide-reaching state-funded international broadcaster.

Critical Moments

In March 2018, RT, as well as Sputnik, attempted to disrupt the Western discourse on the chemical attack on Sergei and Yulia Skripal, who were poisoned with Novichok nerve agent in Salisbury, UK. This disruption involved flooding the narrative space with false or malign narratives to undermine trust in Western news outlets and governments. Ramsay and Robertshaw generated evidence to this claim in their study of the 735 RT and Sputnik publications in the month immediately following the poisoning.^[6] Their research details 138 separate and contradictory narratives explaining the incident, including attacks on Western motives, explanations of the origins of the nerve agent,

and brazen conspiracy theories.^[7] Such narratives include describing the investigation as a “witch hunt” and the UK’s response as illegal; 20 narratives about Novichok, including that it could originate from the UK, US, Ukraine, Iran, or a number of other European states; 16 narratives about the Skripals, explaining the poisoning by alleging links to organised crime, to claims that Yulia Skripal brought the nerve agent into the UK and that the Skripals were never poisoned; 7 conspiratorial narratives, including that the poisoning was conducted by the UK or an intelligence agency of a third country in order to harm Russia.^[8] These data confirm that RT conducts subversion campaigns, which Kuleshov defines as “spreading disinformation among the populations about the work of state bodies, undermining their authority, and discrediting administrative structures.”^[9]

The campaign’s sophistication is notable in its adaptation to Western developments on the case. For example, following then Prime Minister Theresa May’s 12 March speech to the UK Parliament which attributed the Novichok nerve agent to Russia, RT responded with a flood of narratives contesting the origins and existence of Novichok and presenting the poisoning as a Western political stunt. These narratives often were promoted by high-ranking Russian government officials, such as Sergey Lavrov, Dmitry Peskov, and Maria Zakharova, which generated extensive mainstream UK media coverage. Ramsay and Robertshaw describe this as “the most successful means by which pro-Russian narratives were inserted into Western news outlets.”^[10] A key element of this success was the high quantity of publications, which deluged the total narrative space, priming their leak into mainstream discourse.

Such narrative flooding exercises are typical of RT during critical moments. In 2014, when Russia annexed Crimea, RT unleashed a similar campaign of disinformation, accusing Ukrainian demonstrators of Nazi sympathies and ignoring the Ukrainian government’s point of view.^[11] This caused such strain among the news anchors that Liz Wahl quit live on air, refusing “to be part of a network funded by the Russian government that whitewashes the actions of Putin.”^[12]

Non-Critical Periods

During non-critical periods, news reports typically are more subdued and RT functions as a normal news agency seemingly committed to reporting quotidian items that would arouse no suspicions of a clandestine political agenda, which RT often takes to a point of surreal mundanity, assigning undue attention to trivial news items. For example, on August 6, 2019, the top RT headline commented on outrage at British businessman Lord Alan Sugar’s mockery on Twitter of Labour politician Jeremy Corbyn.^[13] Shortly after, the RT headlines praised a 21-year-old’s attempt to install a bionic eye for himself in Vladivostok.^[14] These bizarre areas of focus for any news outlet are more than bizarre for a channel whose mission is to “acquaint the international audience with the Russian point of view” on “major issues of our time.”^[15]

However, Glenny further observes that “the annoying thing about RT is that some of the reporting is very good and genuine.”^[16] RT interviews host politicians from across the political spectrum, from George Galloway, who has his own show, to Nigel Farage. RT can provide updates to basic political developments much like the BBC or CNN. In addition, RT looks like any normal western news outlet. Pomerantsev has noted that the channel has “the thumping music before the news flash, the earnest pretty newscasters, the jock-like sports broadcasters.”^[17] One could interpret this as evidence that RT is simply just another news outlet.

Disguise

Yet RT's Simonyan herself concedes that this image of normality masks the true design of RT. In an interview in 2012 with the Russian daily *Kommersant*, she justified RT as a necessary taxpayer expense for “conducting the information war [...] against the whole Western world.”^[18] Simonyan developed her vision of a nuanced impression of RT, which projects normality during journalistic lulls interspersed between narrative floods, such as those identified following the Skripal poisoning: “it's impossible to start making a weapon only when the war already started!” Like a proud parent, Simonyan even declares that this information serves as an adjunct to the Ministry of Defence. The element of disguise is crucial to this model.

In 2013, Simonyan expanded on the importance of disguise in another interview with a Russian online newspaper, *lenta.ru*.^[19] After reaffirming her vision of RT as “a weapon like any other,” to be “used in critical moments.” she insisted that RT does not aim “to start a revolution in the USA,” which to her would be “laughable and crazy.” Rather, Simonyan said, RT aims “to conquer an audience.” She continues, “[i]n a critical moment we'll already have grown our audience, which is used to come to us for the other side of the truth, and of course we'll make use of that.” Simonyan's words reveal RT's elaborate system of disguise, with the channel fronting as a normal news channel in order to recruit a trusting audience that may be exploited during ‘critical moments.’

Simonyan also explained why it was the 2008 Georgian War that brought home to Russia the importance of disguise in her *Kommersant* interview, where she describes the lessons of the conflict, which was seen by the Kremlin as a military victory but a propaganda defeat: “There weren't enough, and there aren't enough, English-speaking talking heads. People who understood how and why they should go on air with CNN, and how to behave in a studio so they would not get their throats torn out by Western journalists. As a result, Russia looked so pale compared to the Georgians, it broke my heart. [...] It's as if we suddenly realised that there are nuclear weapons in the world and rushed to develop them. This was the main mistake.” The interviewer then asks: “Have any lessons been learned? Is there an anti-crisis mechanism? Is there any understanding that it is necessary to water, for example, the flower called *Russia Today*, so that it will grow into a mighty tree, and could be used as an information cudgel at need?” Simonyan responds, “I think so. [...] In 2008, it became absolutely

clear to everyone why this is needed, why we need such a thing as an international television channel representing the country.” Simonyan here identified the components of the disguise. “English-speaking talking heads” blend in with their BBC or CNN counterparts, along with individuals who know how to present genuine journalism during non-critical periods and thereby avoid “getting their throats torn out.” Six years after the interview, following the Skripal poisoning, the “mighty tree” of Russia’s information weapon stood tall.

Before the Georgian War, rather than undermining Western narratives, RT sought instead to promote Russian ones.^[20] Cooper says “when the channel was first created, it was presented as an effort to present news from a Russian perspective. The point now seems to be much more about promoting conspiracy theories.”^[21] For example, the narrative flood that took place after the Skripal poisoning did not take place in the aftermath of the 2006 Litvinenko poisoning. RT was eerily silent on this issue, receiving scathing criticism from the West for their lack of comment on the incident.

In light of Simonyan’s comments, RT’s guise of normality becomes more obviously a mimic of Western news outlets comprising various strata. The stock news items about fury at Lord Sugar’s tedious tweets or outlandish tales about bionic eyes are imitations of stock news items, creating a hyperreal depiction of journalism, in which the norm is more normal than normal. The slick transitions and graphics seem over-the-top, closer to stage directions than to genuine production cues. During critical moments, RT’s flooding of the narrative space manufactures a blurring between fiction and reality for its conditioned audience. True to Kuleshov’s theory on subversive campaigns, RT spreads “disinformation among the populations about the work of state bodies, undermining their authority, and discrediting administrative structures.”^[22]

However, Simonyan’s statements about RT are markedly more reserved when talking to Western journalists: typically, she reverts to claiming that it conveys “a Russian viewpoint on major global events.” In her 2013 interview with *Der Spiegel* she claimed that RT seeks to prove “that there are more stories out there than the 10-a-day that you usually encounter” on CNN and the BBC.^[23] Shortly after, she interrupted and evaded the reporter’s challenge that “many are comparing [RT] to the Ministry of Defense.” In her 2016 interview with the *Financial Times*, she similarly claimed “that mainstream western TV channels, especially CNN and ABC, show the same thing” as RT.^[24] With Western journalists, and hence Western audiences, Simonyan avoids describing information weapons and deception campaigns. This may cause her to believe that Western audiences will not hear of her near-gloating comments in Russia about the efficacy of RT’s disguise with Western audiences.

Giles represents a popular school of thought that views Russian subversion campaigns like this as “broadly recognisable as reinvigorated aspects of subversion campaigns from the Cold War era and earlier.”^[25] This article indicates that RT is part of a more sophisticated strategy than its Cold War predecessors, especially in its ability to adapt according

to past failures. The station is an advancement from *Pravda*, the Soviet Communist party newspaper, or *Radio Moscow International*, which produced easily identifiable propaganda.^[26] This strengthens Galeotti's conclusion that "Russia is clearly seeing the kinetic and the non-kinetic as 'interchangeable and mutually supporting,' moving away from the traditional Western assumption that 'subversion, deception, and the like' are all 'force multipliers' to the combat arms, not forces in their own right."^[27]

RT's inability to host experts, however, betrays an otherwise persuasive disguise. The channel claims that all guests are diligently vetted: "We care a lot about their credibility. We often invite commentators with alternative views who are not welcome on mainstream stations. Some are quite renowned, such as [Marxist philosopher] Slavoj Žižek."^[28] Some of the most perplexing items feature 9/11 truthers, UFO sightings, and celebrities like Steven Seagal and Pamela Anderson serving as experts. Anderson even appeared on RT to defend Julian Assange against rape charges. In the wake of the 2017 Manchester bombing, RT invited for comment two obscure Western journalists and a serial apologist for Syrian President Bashar Assad. All blamed the attack on Western foreign policy in the Middle East. This issue looks set to worsen, as more legitimate experts and commentators vow to stay away from RT. This illustrates that, upon scrutiny, RT's image of authenticity is betrayed by its inability to host legitimate experts.

Engagement

Aside from its flaws, an estimation of RT's success in attracting an audience should dictate an appropriate response from the West. Engagement is a quantifiable factor which, to some degree, indicates success at gaining an audience, many of whom likely perceive the outlet as credible. RT's popularity on *YouTube* indicates its success at audience recruitment appears to make up for the attention deficit on television. RT is the most engaged news network on *YouTube*, with more than 10 billion views across its channels and over 4 million subscribers. The *YouTube* channel uploads segments from its television channels, amplifying them to the vast audience. This is largely due to RT's practice of purchasing the rights to sensational footage, for instance, that of Japan's 2011 tsunami, and repackaging them with its logo. Though this indicates that its online success owes to dubious tactics, the success nonetheless strengthens RT's disguise.

RT news channels have also expanded at a rapid pace in the last 15 years. Al-Yaum (RT Arabic) was launched in 2007, while RT Actualidad (RT Spanish) followed suit in 2009. In 2011, RTDOC was launched alongside RUPTLY, a video news agency started with subsidies from Moscow to offer professionally produced videos at affordable prices to broadcasters. These both provide even more material to attract a trusting audience during non-critical periods. RT is now located in 16 countries with bureaus in 21 cities, including Washington, New York, London, Paris, Kiev, New Delhi, Cairo, and Baghdad. RT's London office is remarkably luxurious, looming large over Big Ben and the MI5 and MI6 headquarters. The more RT grows, disguised

as a genuine news outlet, the greater the engagement, and the greater its success in recruiting a trusting audience.

But even a modest trusting audience poses a risk of societal harm, given the toxicity of RT publications during critical moments. In 2016, the “Pizzagate” conspiracy mired Hillary Clinton’s election campaign. This groundless theory claimed that a paedophilia ring linked to members of the Democratic Party had been discovered through Clinton campaign manager John Podesta’s emails, published by *WikiLeaks* in 2016. The theory alleged the emails contained code words for paedophilia and human trafficking, naming Comet Ping Pong restaurant as a meeting ground. Ben Swann, a former RT contributor who ran his own media outlet entertained the claims, alongside social media platforms and forums. After admitting the absence of any mention of trafficking or paedophilia in the emails, Swann said “there are dozens of what seem to be strangely worded emails about pizza and handkerchiefs. Self-described online investigators say that those words in the emails about pizza, and the talk of handkerchiefs is code language used by paedophiles.”^[29]

The laughable case took a serious turn on December 4, 2016, when Edgar Maddison Welch walked into Comet Ping Pong with a loaded AR-15 assault rifle and a loaded .38 calibre revolver. While inside the restaurant, which was crowded with customers, including children, Welch fired the rifle multiple times and threatened staff. District Court proceedings concluded that Welch was “motivated, in part, by unfounded rumours concerning a child sex-trafficking ring that was being perpetrated by high-profile individuals” at the restaurant.^[30] Whilst the vast majority of the public viewed the Pizzagate conspiracy as ludicrous, a single believer can wreak havoc, so large audiences are not always necessary in order for an information weapon like RT to inflict serious damage upon society; disguise only needs to convince one person.

The statistics, however, indicate that RT has attracted a sizable faithful audience, thus maximising its devastating potential as an information weapon during critical moments. As McFaul, US ambassador to Russia under Obama, comments, “there is a demand in certain countries for this alternative view, an appetite, and we arrogant Americans [or Westerners] shouldn’t just think that no one cares.”^[31] Especially when one considers the stormy forecast for the future of journalism. The rise of DeepFake, a highly realistic manipulation of audio or video, is of great concern because this technology is increasingly accessible and increasingly difficult to detect.^[30] RT has already demonstrated that it is quick to harness the latest technological advancements. In 2016, RT pioneered the first 360-degree HD video from aboard the International Space Station, while RT360, a special app for delivering 360 content, won the Short Award for Best Photo and Video App in 2017. An RT publication of a DeepFake video in which, for instance, Theresa May revealed to a colleague a plan to poison Sergei Skripal in Salisbury is a sobering thought for journalism and international relations. The image of a volatile adolescent RT is startling, the prospect of the organization in its maturity is even more alarming.

Response

The West must act robustly. In the UK, Ofcom fined RT £200,000 in 2019 for failing to comply with rules on impartiality.^[33] This was largely based on the current affairs programmes RT aired between March 17 and April 26, which failed to “preserve due impartiality,” mostly in relation to the Skripal poisoning. That confrontation followed a series of Ofcom-RT disputes over violating the UK broadcasting code,^[34] including sanctions in 2015 over a “series of misleading and biased articles” about BBC coverage, and requiring RT to broadcast a summary of Ofcom’s findings.^[35]

These penalties appear ineffective. Ofcom has found more RT programmes guilty of partiality than those of any other broadcaster.^[36] Yet RT has continued to subvert journalistic integrity during critical moments in recent years, just as following the Skripal poisoning. On 20 July 2019, for instance, large protests in Moscow demanded that opposition candidates be allowed to register for municipal elections in Moscow. RT grossly understated the crowd size as 12,000,^[37] which multiple Western media outlets, including BBC and Reuters, reported at a minimum of 20,000.^[38] The Digital Forensics Lab, a testament to the value of open-source research tools, corroborated the crowd density and clear boundaries of the crowd with the use of Google Maps satellite imagery and the MapChecking online tool to precisely measure that the protest more likely at 22,000.^[39]

Given these repeated offences, removing RT’s broadcasting licence both in the UK and in all other affected countries is a possibility. In 2018, some in the UK House of Commons urged the more drastic penalty of removing RT’s licence.^[40] On March 13, 2018, Ofcom suggested it could review RT’s licence, “should the UK investigating authorities determine that there was unlawful use of force by the Russian State against the UK” in Salisbury.^[41] In July 2019, RT and *Sputnik* were banned from a media freedom conference in London for playing an “active role in spreading disinformation.”^[42] Thus even journalists—usually among the strongest of champions of free speech—may be reaching the end of their patience.

The UK would not be the first European county to ban the broadcaster. In 2014, the business news-focused RBK-TV joined a growing list of Russian channels banned in Ukraine.^[43] The National Television and Radio Broadcasting Council of Ukraine said the move was made “in the interest of information security,” and, specifically, because the channel violated the European Convention on Transfrontier Television and current legislation in Ukraine. In 2015, Moldova’s Coordination Council on Television and Radio (CCA) banned the Russian channel Rossiya 24 permanently,^[44] stating that the station, and several others like it, constantly distorted facts and manipulated public opinion in stories covering annexation of Crimea. In March 2019, Latvia’s National Electronic Media Council (NEPLP) imposed a three-month ban on the retransmission of Russian language channel Rossiya RTR.

Relations in recent years between the West and Russia have been more strained since the end of the Cold War, and RT is among the issues of contention. The history described above reveals why disguise is a key element of RT's tactics of recruiting and then manipulating a trusting audience during critical moments. This article attempts to more deeply analyze RT than has occurred to date, with direct reference to RT content, as well as journalists' interviews with Margarita Simonyan, which support the interpretation of RT as an information weapon. This situates RT within a wider conversation of the anti-West subversive campaigns of Putin's Russia as espoused by Kuleshov. RT's disregard for lesser punitive measures issued by the UK would also strongly support the revocation of RT's broadcasting licence by Western nations, which not only would remove RT from television screens, but could lead to the closure of RT's overseas offices, thereby undermining RT's ability to publish articles and online content. Equally important, this would publicly unmask RT as the Russian information weapon. In the face of public criticism, this would undo the powerful element of disguise, along with the negative effects of RT's upon Western society. Simultaneously, countries taking this action would demonstrate solidarity and thereby strengthen international ties around the democratic values of a free press. 🛡️

NOTES

1. A multilingual selection of journalistic receptions of RT: T. Dowling, '24-hour Putin people: my week watching Kremlin 'propaganda channel' RT' *The Guardian*, March 29, 2017, <https://www.theguardian.com/media/2017/nov/29/24-hour-putin-people-my-week-watching-kremlin-propaganda-channel-rt-russia-today>, accessed August 6, 2019; A. Macho, 'Der Propaganda-Sender des Kremls in Deutschland' *Handelsblatt*, November 21, 2014, <https://www.handelsblatt.com/unternehmen/it-medien/russia-today-der-propaganda-sender-des-kremls-in-deutschland/11016084.html>, accessed August 7, 2019; S. Lobo, 'Putins Geniestreich' *Spiegel Online*, November 28, 2018, <https://www.spiegel.de/netzwelt/netzpolitik/wladimir-putins-wirkmaechtige-propaganda-in-sozialen-medien-a-1240829.html>, accessed August 7, 2019; J. O'Sullivan, 'Russia Today is Putin's weapon of mass deception. Will it work in Britain?' *The Spectator*, December 6, 2014, <https://www.spectator.co.uk/2014/12/the-truth-about-russia-today-is-that-it-is-putins-mouthpiece>, accessed August 7, 2019; T. Sculthorpe, 'Kremlin mouthpiece RT faces three more Ofcom investigations into whether it broadcasts pro-Putin propaganda' *Mail Online*, May 21, 2018, <https://www.dailymail.co.uk/news/article-5753461/Kremlin-mouthpiece-RT-faces-three-Ofcom-investigations.html>, accessed August 7, 2019; A. Troianovski and J. Warrick, 'Agents of doubt: How a powerful Russian propaganda machine chips away at Western notions of truth' *The Washington Post*, December 10, 2018, <https://www.washingtonpost.com/graphics/2018/world/national-security/russian-propaganda-skripal-salisbury>, accessed August 7, 2019; M. Weiss, 'Russia's Propaganda Blitzkrieg' *The Daily Beast*, October 4, 2017, <https://www.thedailybeast.com/russias-propaganda-blitzkrieg>, accessed August 7, 2019.
2. On RT's use of conspiracy theories as a Russian diplomacy tool, see I. Yablokov, 'Conspiracy Theories as a Russian Public Diplomacy Tool: The Case of *Russia Today* (RT)' in *Politics*, 2015, Vol. 35, 3-4, 301-315; On RT's presentation of Russia, see G. Miazhevich, 'Nation branding in the post-broadcast era: The case of RT' in *European Journal of Cultural Studies*, 2018, Vol. 21.5, 575-593.
3. 'About RT,' <https://www.rt.com/about-us>, accessed August 9, 2019.
4. N. Von Twickel, 'Russia Today Courts Viewers With Controversy' *Russia Beyond*, March 23, 2010, https://www.rbth.com/articles/2010/03/23/230310_rt.html, accessed August 6, 2019.
5. M. Bodner, M. Kupfer, and B. Jardine, (2017) 'Welcome to The Machine: Inside the Secretive World of RT' *The Moscow Times*, June 1, 2017, <https://www.themoscowtimes.com/2017/06/01/welcome-to-the-machine-inside-the-secretive-world-of-rt-a58132>, accessed August 9, 2019.
6. Narratives, for the purpose of the study, were identified as 'any statement within an article that offers a coherent explanation of the circumstances leading to the poisoning, or the motives of actors involved in the event or its aftermath'; G. Ramsay and S. Robertshaw (2018), *Weaponising news: RT, Sputnik and targeted disinformation*, The Policy Institute, King's College London, 128-135; the study used Steno, an open source article analysis tool, <http://stenoproject.org>, accessed August 7, 2019.
7. Ramsay and Robertshaw, *Weaponising news*, 27.
8. *Ibid.*, 28-31.
9. Yu. Kuleshov, et al., 'Информационно-психологическое противоборство в современных условиях: теория и практика' (Information-Psychological Warfare In Modern Conditions: Theory And Practice) in *Vestnik Akademii Voyennykh Nauk*, 2014, 46, No. 1, 106.
10. Ramsay and Robertshaw, *Weaponising news*, 22.
11. B. Nimmo, 'Question That: RT's Military Mission' *Digital Forensic Research Lab*, January 8, 2018, <https://medium.com/dfrlab/question-that-rt-s-military-mission-4c4bd9f72c88>, accessed August 7, 2019.
12. RT America, 'RT America's Liz Wahl Resigns Live on Air', 2014, <https://www.youtube.com/watch?v=2h79v9uirLY>, accessed August 9, 2019.
13. RT, 'Galloway blasts Lord Sugar for 'sacrilegious mockery of Christian martyrs,' asks Pope to intervene' *RT News*, August 2, 2019, <https://www.rt.com/uk/465657-galloway-sugar-skulls-corbym>, accessed August 8, 2019.
14. E. Neskarov, 'The Transhumanist: Russian student who lost sight after explosion developing bionic eyes for himself' *RT News*, August 6, 2010, <https://www.rt.com/news/465859-blind-bionic-prosthetic-nekrasov-russia>, accessed August 8, 2019.
15. 'About RT,' <https://www.rt.com/about-us>, accessed August 9, 2019.
16. T. Dowling, '24-hour Putin people: my week watching Kremlin 'propaganda channels' RT.' *The Guardian*, November 29, 2017, <https://www.theguardian.com/media/2017/nov/29/24-hour-putin-people-my-week-watching-kremlin-propaganda-channel-rt-russia-today>, accessed August 7, 2019.

NOTES

17. P. Pomerantsev, *Nothing Is True and Everything Is Possible: Adventures In Modern Russia*, Faber & Faber, 2017, 89; J. O'Sullivan, 'Russia Today is Putin's weapon of mass deception. Will it work in Britain?' *The Spectator*, December 6, 2014, <https://www.spectator.co.uk/2014/12/the-truth-about-russia-today-is-that-it-is-putins-mouthpiece>, accessed August 7, 2019.
18. A. Gabuev, 'Нет никакой объективности' ('There is no objectivity'), *Kommersant*, July 4, 2012, <https://www.kommersant.ru/doc/1911336>, accessed August 7, 2019; archived: <http://archive.is/Vy4i0>, accessed August 7, 2019; English translation: B. Nimmo, 'Question That: RT's Military Mission' Digital Forensic Research, January 8, 2018, <https://medium.com/dfrlab/question-that-rt-s-military-mission-4c4bd9f72c88>, accessed August 7, 2019.
19. I. Azar, '«Не собираюсь делать вид, что я объективная» Интервью с Маргаритой Симоньян' ("I'm not going to pretend that I'm objective," an Interview with Margarita Simonyan), *lenta.ru*, March 7, 2013, <https://lenta.ru/articles/2013/03/07/simonyan>, accessed August 7, 2019; archived: <http://archive.is/RzLyk>, accessed August 7, 2019; English translation: B. Nimmo, 'Question That: RT's Military Mission' Digital Forensic Research Lab, January 8, 2018, <https://medium.com/dfrlab/question-that-rt-s-military-mission-4c4bd9f72c88>, accessed August 7, 2019.
20. M. Bodner, M. Kupfer, and B. Jardine, 'Welcome to The Machine: Inside the Secretive World of RT' *The Moscow Times*, June 1, 2017, <https://www.themoscowtimes.com/2017/06/01/welcome-to-the-machine-inside-the-secretive-world-of-rt-a58132>, accessed August 9, 2019.
21. M. Bodner, M. Kupfer, and B. Jardine, 'Welcome to The Machine: Inside the Secretive World of RT.'
22. Yu Kuleshov, et al., Information-Psychological Warfare In Modern Conditions, 106.
23. B. Bidder, "The West Never Got Over the Cold War Stereotype" *Spiegel Online*, August 13, 2013, <https://www.spiegel.de/international/world/spiegel-interview-russia-today-editor-in-chief-margarita-simonyan-a-916356.html>, accessed September 13, 2019.
24. M. Seddon, 'Lunch with the FT: Kremlin media star Margarita Simonyan' *Financial Times*, July 18, 2016, <https://www.ft.com/content/7987e5c2-54b0-11e6-9664-e0bdc13c3bef>, accessed September 13, 2019.
25. K. Giles, *Handbook of Russian Information Warfare*, NATO Defense College, 2016, 24; see also, V. Madeira, 'Haven't We Been Here Before?', *Institute of Statecraft*, 30 July 30, 2014, <http://www.statecraft.org.uk/research/russian-subversion-havent-we-been-here>, accessed August 7, 2019; and S. Oates, The Neo-Soviet Model of the Media' in *Europe-Asia Studies*, 2007, Vol. 59, No. 8, 1279-1297.
26. For information on Soviet propaganda, see H.D. Lasswell, 'The Strategy of Soviet Propaganda' in *Proceedings of the Academy of Political Science*, 1951, Vol. 24, No. 2, 66-78; S. Luehrmann, 'THE MODERNITY OF MANUAL REPRODUCTION: Soviet Propaganda and the Creative Life of Ideology' in *Cultural Anthropology*, Vol. 26, No. 3, 363-388.
27. M. Galeotti, Hybrid, ambiguous and non-linear? How new is Russia's 'new way of war'?' *Small Wars & Insurgencies*, 2016, Vol. 27, No. 2, 291.
28. M. Bodner, M. Kupfer, and B. Jardine, 'Welcome to The Machine: Inside the Secretive World of RT.'
29. R. Ho, 'CBS46' Ben Swann fired after attempt to bring back Reality Check' *AJC*, January 29, 2018, <https://www.ajc.com/blog/radiotv/cbs46-ben-swann-fired-after-attempt-bring-back-reality-check/NeAW6LA1crpuxoGqmszkKP>, accessed August 9, 2019.
30. United States of America vs Edgar Maddison Welch, 18 U.S.C. § 924(b) *United States District Court for the District of Columbia*, 2016, <https://arstechnica.com/wp-content/uploads/2016/12/pizzagatewelchfederal.pdf>, accessed August 9, 2019.
31. Quoted in S. Erlanger, 'Russia's RT Network: Is It More BBC Or K.G.B.?' *The New York Times*, March 8, 2017, https://www.nytimes.com/2017/03/08/world/europe/russias-rt-network-is-it-more-bbc-or-kgb.html?ref=collection%2F-sectioncollection%2Fworld&action=click&contentCollection=world®ion=rank&module=package&version=highlights&contentPlacement=1&pgtype=sectionfront&_r=0, accessed August 7, 2019.
32. For the startling possibilities of DeepFake, see H.K. Hall, 'Deepfake Videos: When Seeing Isn't Believing' in *The Catholic University Journal of Law & Technology*, 2018, Vol. 27, 1, 51-77; T. Kwok, 'More Than Meets The Eye: Deepfake Technology and the Erosion of Public Trust' in NATO Association of Canada, July 8, 2019, <http://www.natoassociation.ca/more-than-meets-the-eye-deepfake-technology-and-the-erosion-of-public-trust>, accessed August 9, 2019; M. Maras and A. Alexandrou, 'Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos' in *The International Journal of Evidence & Proof*, 2018, Vol. 23, 3, 255-262.

NOTES

33. Ofcom 'Ofcom fines RT £200,000' *Ofcom*, July 26, 2019, https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2019/ofcom-fines-rt?utm_source=twitter&utm_medium=twitter&utm_content=mobile%2520handsets.
34. B. Nimmo, 'Ofcom And RT: The Background' *Digital Forensic Research Lab*, March 14, 2018, <https://medium.com/dfr-lab/ofcom-and-rt-the-background-1cbeeab77c6b>, accessed August 6, 2019.
35. J. Jackson, 'RT sanctioned by Ofcom over series of misleading and biased articles' *The Guardian*, 21 September 21, 2015, https://www.theguardian.com/media/2015/sep/21/rt-sanctioned-over-series-of-misleading-articles-by-media-watch-dog?CMP=tw_t_a-media_b-gdnmedia, accessed August 5, 2019.
36. M. Bodner, M. Kupfer, and B. Jardine, 'Welcome to The Machine: Inside the Secretive World of RT.'
37. E. Odinokov, 'Protesters rally in Moscow over barring of opposition candidates from city council election' RT, July 20, 2019, <https://www.rt.com/russia/464645-protest-rally-moscow-election>, accessed August 5, 2019.
38. BBC News, 'Moscow protest: Thousands demand fair elections' *BBC News*, July 20, 2019, <https://www.bbc.co.uk/news/world-europe-49057803>, accessed August 5, 2019; T. Balmforth, 'Russian opposition vows to hold Moscow protest despite crackdown' Reuters, July 25, 2019, <https://www.reuters.com/article/us-russia-politics-opposition/russian-opposition-vows-to-hold-moscow-protest-despite-crackdown-idUSKCNIUK1B5>, accessed August 5, 2019.
39. B. Nimmo, 'Kremlin Outlets Downplay the Size of the July 10 Protests in Moscow' *Digital Forensic Lab*, July 29, 2019, <https://medium.com/dfrlab/kremlin-outlets-downplay-the-size-of-the-july-20-protests-in-moscow-56a36aa5b9f5>, accessed August 4, 2019; MapChecking available from: <https://www.mapchecking.com>, accessed August 9, 2019.
40. BBC News, 'Russian spy: MPs want Russian TV station UK licence 'reviewed'' *BBC News*, March 12, 2018, <https://www.bbc.co.uk/news/uk-wales-43377833>, accessed August 3, 2019.
41. Ofcom, 'Statement on RT news channel' *Ofcom*, March 13, 2018, <https://www.ofcom.org.uk/about-ofcom/latest/media-releases/2018/statement-on-rt-news-channel>, accessed August 2, 2019.
42. BBC News, 'Russia's RT banned from UK media freedom conference' *BBC News*, July 9, 2019, <https://www.bbc.co.uk/news/world-europe-48919085>, accessed August 5, 2019.
43. C. Dziadul, 'Moldova bans Russian channel' *Broadband TV News*, May 28, 2015, <https://www.broadbandtvnews.com/2015/05/28/moldova-bans-russian-channel>, accessed August 5, 2019.
44. Ibid.

Combined Information Overlay for Situational Awareness in the Digital-Anthropological Terrain

*Reclaiming
'Information'
for the
Warfighter*

Dr. Zac Rogers

Dr. Emily Bienvenue

INTRODUCTION

As noted in the 2019 *National Intelligence Strategy*,^[1] technology-driven transformation across social, political, and economic domains continues at warp speed. Implications for militaries and their supporting Intelligence Community (IC) have expanded both in scope and complexity. Joint operational planning and evaluation occur in this disrupted and transitional environment, with very little predictable framework capable of guiding practitioners and strategists. This article addresses this discrepancy. The authors introduced and argued for creating a Strategic Engagement Specialist (SES) role in a JFQ article titled *Strategic Army* (October 2019), which concludes that strategic effect in the Information Environment (IE) cannot be achieved through discrete IOs, but rather, with holistic ‘Strategic Engagement’ that reinforces trust.^[2] In that vein, here we introduce practical measures that should be incorporated into doctrine. The article addresses the following overarching questions: How can strategic intent more readily *translate* into a cross-enterprise approach to the IE and, how can that translation be made more discernible and actionable to enterprise-wide decision-makers? To this end, we describe the shortcomings of PMESII with IE shifts. Our proposed analytical framework and toolset augment existing approaches to situational awareness in the Digital Anthropological Terrain (DAT). We explain how scaffolding the operational framework with the Strategic Engagement approach, geared toward building human relationships, is the missing translation piece required to expedite successful IO integration within the Joint Military Appreciation Process (JMAP), and reflect on the implications for doctrine of adding the toolset and methodology we recommend.



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.

For the PMESII Problem

Operational and strategic planners are familiar with the political, military, economic, social, information, and infrastructure (PMESII) taxonomy. For four decades, analysis of PMESII taxonomies and their interplay have been the predominant analytical framework for the repeatable and timely assessment of the changing strategic landscape and operating environment. Indicative of the constant learning undertaken by the national security, intelligence, and defense (NSID) community during the Cold War, this framework seeks to capture the complexity of state behavior, treating states less like billiard balls and more like multi-faceted entities. It reflected the fact that the Cold War was a battle between whole societies for influence on and among the global order fought across multiple fronts. As Ducote notes in a 2010 School of Advanced Military Studies (SAMS) monograph, the basic PMESII schematic has been updated to PMESII-PT with the addition of “physical environment” and “time” and has been accompanied by an array of auxiliary and alternative frameworks favored by various branches of the NSID community.^[3]

Traditionally, each category of analysis was treated as discrete, and each was assigned a branch of the NSID community responsible for that line of effort. A well-known wicked problem for organizations, this tended to obscure complex interactions across categories and almost blinded to emergent properties that arose from these interactions.^[4] As Ducote explains, “Founders of PMESII sought knowledge to untangle the complicated aspects of a system. Then, they wanted to use their findings in the targeting process. However, they did not necessarily seek in-depth meaning and understanding about the complexity of a system.”^[5] As global complexity has markedly increased, particularly with the rise of digital technology and the hyper-connectivity it has enabled, the capacity for the NSID community to muddle through without suffering the serious risks of cognitive blind-spots is in question.^[6] The strategic risk of



Dr. Emily Bienvenue, a Senior Analyst in Joint Operations and Analysis Division of the Defence Science and Technology Group where she provides support to strategic policy and operational planning, is also Adjunct and Research Lead at the Jeff Bleich Centre for the US Alliance in Digital Technology, Security, and Governance at Flinders University of South Australia.

making erroneous assumptions about the implications of complexity, and making hasty actions before fully understanding those implications is well documented.^[7]

The growing awareness of adversarial Information Warfare (IW), and the flow of information through physical and human networks has provided a lens on this process. In practice, though, IW defaults to a means of achieving operational dominance in the physical battlespace through superior Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) with a precursor element of Psychological Operations (PsyOps). C4ISR technological dominance, especially in Cyber and Electronic Warfare (EW) operations, makes PsyOps, alongside the access and control over telecommunications infrastructure and media outlets for Information Operations (IOs), the standard means of producing informational effects under the catch-all of IW. Yet, as later explained, at the operational level these sporadic efforts fall short in the society-centric cognitive war.^[8]

Society-centric, population-centric, and socio-cognitive political warfare, whether interruptions between outbreaks of kinetic Clausewitzian-organized violence or something more enduring, begins to overload the PMESII taxonomy and thus limits the practicality of defaulting to C4ISR dominance when it comes to IW. However enduring or episodic these shifts may be, a gap has opened up. (See Figure 1.)

Real-world examples of this gap are readily forthcoming. In the past 18 months, the NSID community, including Australia, was preoccupied with the contested balance of conventional military capabilities in the East Asian maritime periphery. Policy discussion and media commentary focused on expanding military and para-military maritime capabilities and island-building activities while academic research, and related issues were framed as a threat to conventional sea lane security.^[9] Often characterized as “salami-slicing,” “little blue

men”—the maritime equivalent of Russia’s “little green men” in Crimea and Eastern Ukraine—inch ed their way forward in these waters, crisscrossed by strategically critical sea lanes, careful to avoid triggering the threshold of armed conflict. Maritime diplomacy was often pronounced as the solution to what was broadly understood as a geographically constrained traditional geopolitical struggle over a strategically important thoroughfare. This threat has also been analyzed within various IW contexts,^[10] such as psychological, media, and legal, with the intent to sway public opinion and tip the scales in favor of adversarial narratives in various state-centric institutional forums.^[11]

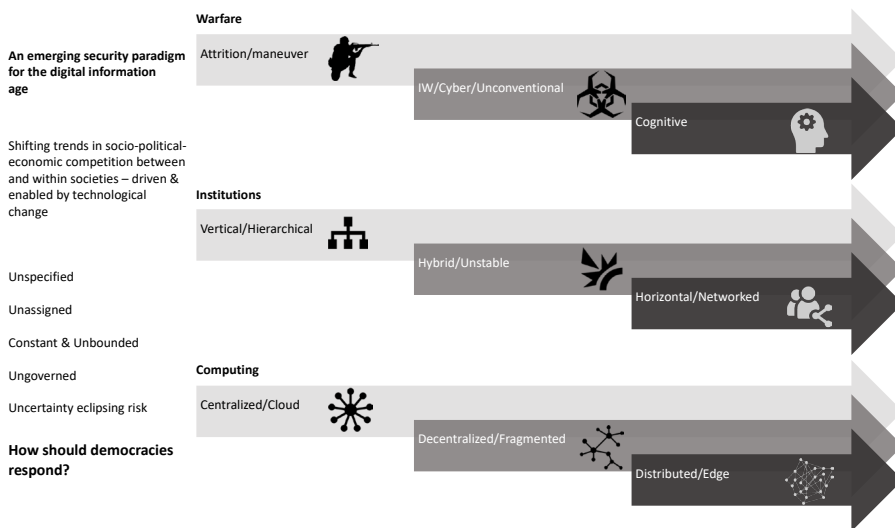


Figure 1. Socio-Cognitive Security©

Retrospective analysis of the IE reveals a more fundamental change in the strategic landscape. At stake in the Indo-Pacific for Australia—beyond access to and control over this strategic maritime space—the socio-cognitive contest^[12] playing out among regional populations. This contest is enabled by access to and control of a Digital Anthropological Terrain (DAT), which is now increasingly pivotal to peace and stability, or “the geopolitics of information” as one Australian analyst called it.^[13] Similar dynamics characterize the Russian campaigns in Crimea, Eastern Ukraine, and across the Middle East.^[14] Moreover, nation-states do not monopolize these trends. Various non-state actors are also exploiting the cognitive blind spots of Western NSID communities.^[15] The offensive component of these society-centric cognitive warfare strategies is designed to undermine the social fabric of open societies, and thus the legitimacy of the rules-based governance of the commons –the foundation of US leadership and power since World War II.^[16] It is also becoming clear that the defensive component is designed to sow enough confusion that it delays and disrupts a coherent, strategic response to this multi-faceted challenge. In practice, however, offensive and defensive components are unified via the fusion of effects facilitated by the participatory nature of digital space.^[17]

The net effect benefits state and non-state actors who see fostering societal chaos as a feature, not a bug, of their strategic competition concept.^[18]

As a recent study observed,^[19] NSID communities seeking a battlefield knowledge edge find themselves embedded in a chaotic contest to unravel the *meaning* associated with that knowledge, and how it is formed and transmitted throughout society—something they are ill-equipped to do. Technology often fails to provide the answers that we seek.

Computers offer humans the promise of speed, efficiency, and precision in sorting and processing information, often at an unacknowledged cost. Providing these effects requires computers to *delete* information. Yet as humans have become socialized into new forms of human-computer interaction, we increasingly accept computational intervention as normal and warranted as it ascends the Cognitive Hierarchy.^[20] Consistent with this cognitive schematic (See Figure 1.1.), we increasingly treat information as mere data, and knowledge as if were mere information. As each threshold dissolves, speed erodes the contextual boundaries between human understanding and statistical inference, leaving two residual consequences: creeping intellectual debt,^[21] and paralyzing confusion.^[22]

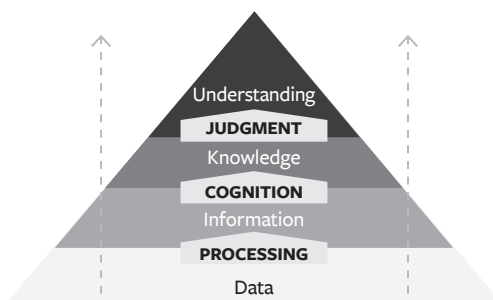


Figure 1.1. Cognitive Hierarchy

As the digital age has enveloped military affairs, and the deluge of data has driven the development of increasingly inscrutable sorting mechanisms known as deep-learning algorithms, humans are set to offload more and more of the cognitive process. Militaries labor under these conditions to pursue the conceptual development and practice of IO. In a 2002 SAMS monograph, Bryan Sparling highlighted a core question for the military in harnessing the digital information age: Are IO an *integration* strategy or are IO a *capability*?^[23] The debate over this question remains unreconciled, with consequences that are accumulating. As Carl Builder noted in 1999, IO as an integration strategy implies a fundamental transformation of our military enterprise—new digital tools would not only alter military roles and missions; they would alter the primary purposeful activity of the modern military.^[24]

IO as a capability implies an enterprise applying new tools to its existing roles and missions. As the answer to this question sorts out, militaries are hedging. In some cases, as Sean Lawson has observed, radical responses to the digital information age have been formulated and deployed on controversial intellectual foundations, with significant strategic consequences.^[25]

Pre-empting this discrepancy in 2002, Sparling challenged the US DoD to “identify and articulate a relevant and theoretically sound definition of information before it can develop practical and effective doctrine for warfighting in the 21st century,” asserting that IO must transcend the dichotomy of integration vs. capability.^[26] Sparling’s “Sentient Information Theory” urged DoD to interweave IO throughout the military enterprise and, crucially, to understand both the *internal* and *external* effects of this weaving.^[27] In other words, as the military incorporates IO for effects in the world, IO will have effects on the military.

It is also safe to say the digital information age did not wait for such a definition to be socialized across the NSID. To date, while noted in the 2018 out-of-cycle *Joint Concept for Operating in the Information Environment* (JCOIE),^[28] nothing like Sparling’s recommendation has made its way into doctrine. Some analysts are alternatively recommending the concept of ‘narrative warfare’.^[29]

But is narrative warfare the appropriate paradigm? Ductote as a response to the PMESII problem urges “identity-based narration” in pursuit of holistic understanding of the OE. He too grapples with the fact that narrative warfare occurs across whole societies which are far more connected through horizontal networks, and thus, that all actions and activities taken by the NSID community and the military services are infused with a narrative whether intended or not. That is, the military may not be interested in narrative, but narrative is interested in the military.

These networks traverse an infrastructure that incorporates government organizations alongside commercial tech companies—media from the mobile device to the submarine cable. Dislocated from its traditional hierarchical position, the increasingly congested narrative warfare hosts fluid and deforming socio-political power structures in which the nation-state’s traditional control power is scattered amidst competing mechanisms and processes causing constant perturbations.^[30] For proponents of narrative warfare, the questions of narrative fratricide, blowback, and the unanticipated side effects of their interventions loom large. Should open democratic societies manipulate the manipulators? Game the gamers? And how would these measures impact the fabric of trust which is so vital to open society? As Kerbel puts it, this calls for states to engage in narrative warfare be an example of “activity masquerading as progress?”^[31] And what other unintended consequences will come of such activity?

For NSID purposes, changes in the world require corresponding changes to the map and how it is produced and disseminated. The PMESII framework must be augmented to capture the disruptive social and political effects of rapid technological change to arm decision-makers with the timely, targeted information that reduces uncertainty. The digital age consists of an interactive medium that requires continuous up-to-date mapping and deconflicted operational planning that avoids informational fratricide^[32] and otherwise achieves strategic alignment within defense organizations. As stated in *Military Strategy in the 21st Century*: “These interactions are not reducible to the physical confines of the land domain, which tend to focus on geography

and terrain features. They represent a web of networks that define power and interests in a connected world. The state that best understands local contexts in all dimensions and builds a network around relationships harnessing local capacity is more likely to win the 21st-century struggle for the flanks.”^[33]

Practitioners agree. U.S. Army Cyber Brig. Gen. Richard Angle in July 2019 asserted the following:

Army Cyber wants to enrich the concept of Multi-Domain Operations through the development of, or enhancing of, information warfare or maneuver in the Information Environment concept, and the further development, integration, and sync of information warfare capabilities across the full range of military operations in competition and conflict. (We are) expanding the concept of persistent engagement in cyberspace to persistent engagement in the Information Environment.^[34]

Lt. Gen. Stephen Fogarty spoke of “a recognition that 1s and 0s moving in cyberspace are not necessarily turning things on or turning things off, but those 1s and 0s are moving information. And that information is changing behaviors and beliefs, and it more powerful than turning things on and turning things off.”^[35] If, after two decades of clarion calls, the NSID community is now resolved to embrace what many have framed as an imperative fraught with uncertainty, the NSID community must manage expectations of risk and opportunity and establish clear strategic goals in advance.

Situational Awareness in the Digital Anthropological Terrain (DAT)

Digital age situational awareness for planning, executing, and learning from military operations requires enhanced cartography. Systems and personnel at home or leaving domestic shores enter an environment comprised of the five familiar domains of land, sea, air, space, and cyberspace. Each of these domains has been carefully mapped using sophisticated ISR platforms, systems, and analysis designed to provide a dominating edge at the command level. Yet, as shown above, digital saturation and hyper-connectivity now link across these domains. This creates complex cross-domain interdependence and emergent properties and introduces non-linearity to the risk-uncertainty distinction thereby challenging prediction, preparedness, and resilience. Operational surprise can occur as a hostile narrative, easily prosecuted by fleeting, deniable, inexpensive, and increasingly automated tools.^[36] Campaign failure can emerge from a growing range of sources, with the effect of reducing command and control to uncoordinated serial reactions to unexpected forces.

Incorporating the two “I’s” of the PMESII taxonomy—infuses the other four domains, thereby improving situational awareness of the machinations of power and influence. Computer scientists, software engineers, network managers, and cybersecurity practitioners well understand the concept of digital stack. This concept has been further developed by theorists and analysts to better understand how technological, social, and political systems shift because of the digital information-networked age.^[37] One chief architect of The Stack is Benjamin Bratton who

captures this radically altered anthropological-technological global environment with a six-layered stack by describing it as a “semi-autonomous, accidental megastructure, governing but not governed, distorting and deforming contemporary political geographies.”^[38]

Many scholars before Bratton argued that digital technologies and human beings should be viewed as an enmeshed matrix of complex dependencies and relations instead of understood within the traditional instrumental human-technology schematic of “user” and “used.”^[39] Latour implored us to recognize the need to understand the human-technological domain broadly as an “anthropological matrix.”^[40] Science and technology historian George Dyson wrote of the emergence of “analogue computing,” where digital computation merges with analogue human behaviors in unpredictable and radical ways.^[41] This discourse, with specific reference to the digital age and operational military affairs, leads us to assign a Digital Anthropological Terrain (DAT).

We seek to re-establish a foothold for operators plagued by uncertainty and to connect operations to strategy. Our response falls somewhere between recommendations by Sparling and Ducote in their 2002 and 2010 SAMS monographs. We aim to respond conservatively, judiciously, and defensively to the foregoing developments without advocating for the implementation of measures that increase the risks of narrative fratricide, blowback, and lost trust. We utilize the digital stack theme to develop an operationally-focused Combined Information Overlay (CIO) to augment the strategic multi-layered analysis of the Digital Anthropological Terrain (See Figure 1.2.). As a framework to map distorted and deformed flows of information and power in any digitally saturated environment, it can aid in augmenting PMESII. The digital stack layers are sites of major consequence—pivotal gateways accommodate influential gatekeepers that control information flow across the digital stack. As a stepping-stone, these sites of cyber-enabled influence are analogous to air-sea-land bubbles—A2/AD pockets whereby a superior conventional joint military force or coalition of forces could seek to exert temporal and spatial denial or control of traffic transiting the relevant zone.^[42]

The historical analogy with familiar air-sea-land domains and the will and capacity of states to deny and control these commons only extends so far into cyberspace.^[43] States face not only a greater diversity of agents both resolved and capable of challenging denial and control of the DAT and the structure of the digital commons, which lends itself to vastly greater exploitation. Loudoun County,^[44] Virginia which, according to its economic-development board, still routes 70-80 percent of global internet traffic,^[45] acts as a digital age Strait of Hormuz in terms of control of the commons, but this analogy is superficial. Translating control into strategic gain is more complex and protean when it comes to information. When crude oil hits the marketplace, the forces of supply and demand assume control—US and allied national security apparatus perform their primary strategic job once extraction, processing, and transit are secured.

In contrast, when digital information hits the marketplace, a wide and ever-shifting range of agents and structures take over. Contrary to many popular accounts, data is not the new oil.^[46]

The supply chains associated with the hardware and software that constitute the digital medium are global, complex, unprotected, and vulnerable. Digital infrastructure from submarine cable landing points to regional telecommunications hubs and local cellular networks is diverse and exploitable. The last 12 inches of the DAT—the human-computer interface—is a congested zone of manipulation employing insights from the cognitive and behavioral sciences for a range of commercial and political ends, both legitimate and nefarious.^[47] The implications of this caldron are only beginning to be understood in terms of impact on socio-political stability,^[48] human well-being,^[49] and the democratic fabric.^[50] Military effectiveness—which ultimately draws all of its resources from society^[51] and is continuously impacted by all societal changes—is deeply implicated.^[52] This means serious augmentation of PMESII for the digital age is critical.

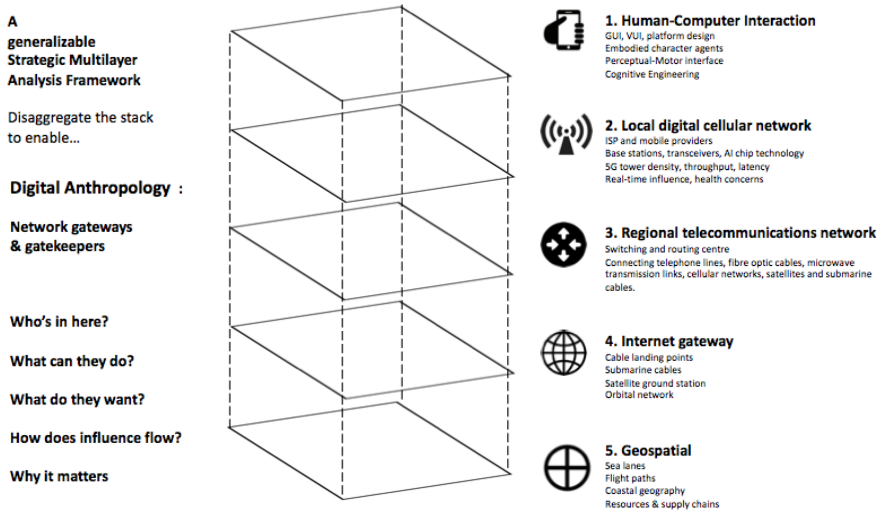


Figure 1.2. Digital Trust©

Disaggregating the DAT

The operation of five digital stack surfaces are both individually consequential, and are also a component of the whole, making the analyst's role pivotal. Adding the digital stack to PMESII brings operational analysis and planning up to speed with the existing operationally important (but still under-appreciated) phenomena; it also will enable foresight in the radically shifting landscape of power and influence the NSID community needs to operate within. The first step in producing a Combined Information Overlay needed for analysis in operational planning and evaluation happens by populating the surfaces described below with information. Open-source information relevant to these surfaces is abundant and should not be overlooked. Once populated, and depending on the nature of the corpus developed, various data tools can help identify sites of unexpected and highly useful information not captured by the PMESII approach. These tools range from a simple web crawler to patterns of connection identified in digital trace

data^[53]—URLs, social media posts, and threads—to more sophisticated digital forensic tools that work with unstructured data to produce statistical inference. The resulting CIO will augment PMESII and assist the strategic analyst who ideally would be proximal across the decision-making structure. As explained below, the analyst populating the stack with information must be mindful of the terrain.

Surface 1. Human-Computer Interface (HCI)

The last 12 inches is the most tactically pivotal and fast-moving surface of the DAT. Humans interact with computers in many ways; the design interface between humans and computers is crucial to facilitating this interaction and has been a growing industry since the mid-1990s.^[54] Desktop applications, internet browsers, every conceivable platform and application on now-ubiquitous handheld mobile devices make use of the graphical user interfaces (GUI) of today. Voice user interfaces (VUI) are used for speech recognition and synthesizing systems, and the emerging multi-modal interfaces allow humans to engage with embodied character agents and virtual assistants in ways not possible with other interface paradigms. HCI has grown insofar as quality of interaction, and in different branching of the purposes of interactions. Instead of designing regular interfaces, the different research branches have focused on different aspects of concepts of multimodality, intelligent adaptive interfaces, and, active interfaces. Each branch is fed continuously with insights and developments emerging from the cognitive sciences over more than three decades.^[55] Innovation is supercharged by dual-use commercial incentives, which keeps political warfare practitioners far ahead of the government’s regulatory and legislative oversight. Command and control must be aware and prepared for adversaries to manipulate, cognitively affecting personnel serving during operations and also on the home front. Measures to protect information assurance between command and personnel—such as repudiable digital record of authenticity using technologies such as blockchain—are readily available.

Surface 2. Local Digital Cellular Network

This surface represents the highly critical last few hundred feet in adversary IO targeting populations. Digital cellular networks are divided into a mosaic of small geographical areas, or cells. Sound and image analog signals are digitized in the mobile device, converted by an analogue-to-digital converter, and transmitted as a stream of bits. All wireless devices in a cell communicate by radio waves with a local antenna array and low-power automated transceiver (transmitter and receiver), over frequency channels assigned by the transceiver from a common pool of frequencies, which are reused in geographically separated cells. Local antennas relate to the telephone network and the Internet by a high-bandwidth optical fiber or a wireless backhaul. Like existing cellphones, when a user crosses from one cell to another, their mobile device is automatically handed off to the antenna in the new cell. The corporate gatekeepers of technology ownership and administration in these networks are critical, and the supply chain of technological components that make the network function are critical to both offensive and

defensive influence. Sound data analysis of API nodes at this surface improves the situational awareness of attempts to manipulate or distort the IE.

Surface 3. Regional Telecommunications Network Backbone

This critical operational surface in terms of routing and switching is the backbone of the regional telecommunications network. It includes telephone lines, fiber optic cables, microwave transmission links, cellular networks, communications satellites, and undersea telephone cables, all interconnected by switching centers facilitating communication among most devices. Originally a network of fixed-line analogue telephone systems, in many countries the backbone is now almost entirely digital at its core and includes mobile and other networks, as well as fixed telephones. Again, ownership and administration of this surface is a critical gateway for routing information to sections of the population targeted for influence. Developing nation-states seeking to enter the digital age are particularly vulnerable to undetected hostile influence that invades the DAT. Commands here can incorporate knowledge of hardware ownership and administration to enhance operational risk awareness and gauge the extent to which regional IT infrastructure is trustworthy.

Surface 4. Internet Gateway

This slower moving, foundational surface is a network of private, public, academic, business, and government networks of local or global scope, linked by a broad array of electronic, wireless, and optical networking technologies. The Internet carries a vast range of information resources and services, such as the inter-linked hypertext documents and applications of the World Wide Web, electronic mail, telephony, and file sharing. Where the nation-state connects to the global Internet via a cable landing station and the cable itself, and in under-developed and sparsely populated archipelagic regions in particular, local satellite infrastructure is obviously a critical gateway with huge operational implications for those who own and administer these technologies.

Surface 5. Geospatial

Geospatial is the strategic surface with the greatest inertia. The increasing ability to capture geographic data is creating an increasingly data-rich environment, including remotely sensed imagery, environmental monitoring systems such as intelligent transportation systems, and location-aware technologies such as mobile devices that report location in near real-time. A geographic information system (GIS) provides platforms for managing these data, computing spatial relationships such as distance, connectivity, and directional relationships between spatial units, and visualizing both the raw data and spatial analytic results within a cartographic context. Also, basic DAT components are dispersed geospatially. The extraction, processing, and transporting of rare earth minerals, and the manufacturing processes to which these minerals are critical inputs, such as the semi-conductor industries which dot the East Asian maritime periphery, represent the geospatially dispersed DAT. Security and control at this surface

are strategic imperatives for the relevant operational command.

DAT Denial vs. DAT Control?

While the DAT cannot be wholly controlled by command, freedom of maneuver can be denied to hostile narratives. Great improvement can be achieved here by the military. By way of analogy, sea denial and sea control are long- and well-understood naval concepts.^[56] For navies, sea denial is the denial of a certain maritime domain to an adversary, with or without access and transit of such area for oneself, whereas sea control denotes the achievement of both. Generally, sea denial is much more readily achievable than sea control, particularly in the era of precision-strike parity.^[57] Sea control may be grasped temporarily during major combat operations but usually cedes to sea denial as forces demobilize and seafarers fall back on a constabulary presence.

The denial versus control contrast deepens in cyberspace to the point of redundancy. DAT control—the capacity to deny digital-anthropological medium usage while freely using the terrain unharried—is nearly impossible, even during major cyber operations. Advocates of engagement in narrative warfare must be able to account for indiscrete boundaries of their interventions, and the consequences of their interventions are multi-directional. Side effects and accidents are unavoidable when intervening in complex anthropological systems—the sciences offer nothing to eliminate this reality. This constraint, and an open society’s heavy reliance on trust as a foundational societal imperative, means that narrative warfare that seeks to manipulate a given section of the population requires a rigorous cost-benefit analysis of long-term strategic effects and a serious dose of prudence and realism.

DAT denial—the capacity to deny free use of the medium to an adversary while not being free to use it unharried—is a much more plausible goal. DAT denial holistically is the force’s foundation of operational cognitive security. Understanding how influence operates through the DAT helps to identify opportunities to deny access to adversaries and gain a small window of advantage. It does not mean offensive cognitive operations always succeed. Information fratricide, the well-established failure rate of covert interventions,^[58] and the emerging ethical constraints on increasingly transparent warfare^[59] present high barriers to ambitions of DAT control. A better approach is to use DAT denial to pursue resilient human relationships by cultivating and reinforcing trust. The authors echo Sparling in advocating for leveraging trust as a heuristic for Strategic Engagement allows information to be wielded not as a narrative weapon but rather to cultivate our preferred environmental condition. Yet the bluntest and generally counterproductive example of DAT denial is an Internet blackout—and states often have opted for this lose-lose option.^[60] It serves, however, as a glimpse of near-future conflict. Augmenting operational security with analogue civil-military human relationships long-term is a win-win. When the lights go out, what else does the enterprise fall back on?

Integrating the DAT into JMAP for Strategic Engagement

JMAP acknowledges Phase Zero scoping and shaping must intersect the phases. The need for

persistent engagement under the Accelerated Warfare concept is the most explicit official acknowledgment of this.^[61] By augmenting PMESII with CIO for situational awareness in the DAT, we provide a structured way to address complexity in the form of recurring updatable analysis with immediate relevance to the decision-maker. As for the JMAP (See Figure 1.3), an in-practice disconnect remains in the ways the arrows connecting Joint Intelligence Preparation for the OE impact on decision-making across the phases, how those decisions connect and align with strategic intent, and how the feedback loops across the phases arm the decision-maker with meaningful information about the operation. Lots of information gets exchanged, but the decision-maker is often left asking “so what?” What is the plot binding each decision, what is the narrative signature that each decision creates?

Strategic Engagement Specialist (SES) role

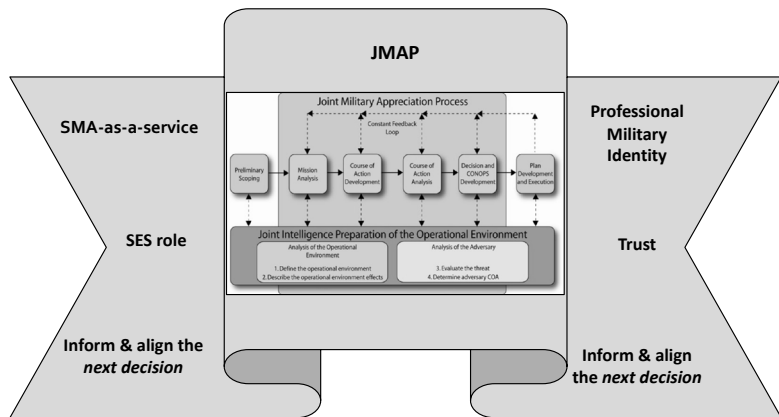
Use **UAI-denial** to mitigate adversarial narratives

Use **Combined Information Overlay for SMA** to equip decision-makers for Strategic Engagement

Augment **Strategic Engagement** with face-to-face trust building and sustainment

Align strategic & operational objectives at each decision point across the enterprise by...

Prioritizing **professional military identity** to connect strategic intent with **information as an environmental condition**



“information as an environmental condition”

Figure 1.3. SMA-as-a-service©

Strategic Engagement is not realized until these arrows inform the decision-maker of key and digestible information. This can be produced in the form of CIO for situational awareness in the DAT, but the question “So what?” remains. This question is answered by referring to DAT denial as the *persistent operational objective* and trust-building as the *environmental condition*^[62] in which strategic intent is pursued. DAT denial and trust connect operational and strategic levels, with the aim of elucidating and facilitating an all-enterprise understanding, as urged by Sparling.

Analysts who exchange OE intelligence with practitioners, and practitioners who cross-reference operational status can access a common understanding of the desired environmental condition of information without requiring an identical flow of intelligence and without receiving identical orders simultaneously from command. Trust as a strategic resource underpins the preferred environmental condition and DAT denial as the preferred operational state. These are the connective tissues that need strengthening in the existing JMAP as it is currently practiced.

Bolstering Professional Military Identity as a Strategic Resource

The role trust plays in today's strategic landscape speaks to the importance of honor and integrity in professional military identity and how the integrity of our service professionals serves as a key ingredient in the fight to protect our democratic societies. Traditionally, our military has been one of our most trusted institutions. In Western democratic societies, and this remains true today. A 2018 Gallup study showed 74 percent of Americans polled trusted the military "a great deal or quite a lot"—the highest of all institutions.^[63] Military professionals are at the coalface of international diplomacy in an era of radical transparency and contested narrative, and so is the foundational backstop of strategic trust. Acknowledgment of such is needed to precipitate greater investment in professional military education to capitalize on values of honor and integrity—a natural strength of the military enterprise—as our best defense against the malign information campaigns of our adversaries.

Professional military identity, a strategic resource, can also help bridge the gap between the strategic integration of IO across the military enterprise and operational decision-making, planning, and evaluation. Tactical technological advances and innovative organizational reform can only get the enterprise so far. The last six inches—the “so what” question confronting the operator amidst a deluge of information, knowledge, and narrative—remains vulnerable to the stifling and paralyzing effects of uncertainty in the cognitive battlespace. Technological and organizational mitigations are necessary but insufficient in the cognitive war. Cognitive security is a construction of the originator—a narrative pushed forward as much as one deduced from the IE. Noting that technological and organizational fixes will never be sufficient even with improvement over time, the key to finding a foothold in the digital age and reclaiming information for the warfighter are the values and identity of the originator with no other choice except to operate in a protean and fluid IE. As noted above and argued for in *Strategic Army*, the military's status, particularly the Army as the societal trusted institution *sine qua non*, is the heuristic around which IO integration at both the strategic and operational levels should be pursued.

CONCLUSION

This article addresses the following questions: How can strategic intent more readily *translate* into a cross-enterprise approach to the IE, and how can that translation be made more discernible and actionable, enterprise-wide, to decision-makers? These are not simple tasks. For more than two decades, scholars and practitioners have underscored the imperative for the military enterprise to adapt to the digital age. The armed forces and their supporting NSID communities have yet to reach the optimum stage where, as Sparling urges, terms and concepts such as IO, IW, and IE are made redundant because the entire military enterprise understands “information” as an *environmental condition*, in the way a seafarer understands seawater or an infantryman the landscape's topography. The CIO introduced here for situational awareness in the DAT represents an overdue retracing of steps for the military with emphasis on operational

security in cognitive war. It should by now be uncontroversial to recognize that the primary contest in cognitive war, as members of the NSID community, is with ourselves.^[64]

But the perennial strategic question is clear: What *conditions* should we be seeking to establish? And, operationally, how should those conditions lead towards the next decision? The fusing of approaches to information in operations and strategy in the digital age cannot succeed without incorporating the way that the originators' operations and strategy create a narrative signature, and how audiences read and receive that signature. The hyper-connected digital age means the audience is global, the signature is mutable and travels at light speed, and control power in the DAT is an increasingly dangerous and self-defeating fantasy. Operators need a foothold for operational security grounded in cognitive security throughout meaningful activities. This means persistence and conservative expectations about how the DAT can be managed.

Digital age realities mean the construction and maintenance of analogue human relationships, in which trust is established as a strategic resource rather than an auxiliary luxury, will remain critical to operational success in the digital age. DAT denial that accompanies human relationships is a capability—its significance to the strategic integration of information across the enterprise is in its proximity to trust as the critical missing translation piece.

Trust in this context is akin to an environmental condition the originator seeks to attain and sustain, not a signature it seeks to exploit. Trust is defensible precisely because it weaves in and out of the human-machine terrain in indiscrete, culturally specific ways. Those seeking to abuse trust and employ it offensively in cyberspace will encounter this constraint. We achieve operational security in the cognitive domain by pushing trust forward not by retreating from it in a race to the bottom with an adversary for whom trust is a non-starter. To this end, we view DAT denial via constantly updated and disseminated CIO; using the framework outlined here should be part of the enterprise-wide doctrine. The JMAP needs an overhaul, not mere augmentation, aligning operations and strategy with an information-relevant environment, thereby reclaiming information for the warfighter. Cultivating and sustaining trust in human relationships strategically aligns the enterprise, and renders it accessible and understandable for decisionmakers at every level. Trust is the core “plot” binding every narrative signature. IO without trust will continue to oscillate between self-defeating and costly at the operational level and will be dangerously corrosive at the strategic level.🛡️

DISCLAIMER

The views expressed below are the authors', and do not represent the official view of the Australian Defense Department.

NOTES

1. Office of the Director of National Intelligence, “National Intelligence Strategy of the United States of America” (United States Intelligence Community, 2019), https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf?utm_source=Press%20Release&utm_medium=Email&utm_campaign=NIS_2019.
2. Emily Bienvenue and Zac Rogers, “Strategic Army: Developing Trust within the Cognitive Battlespace,” DST Group Discussion Paper (Edinburgh, South Australia: Joint Operations and Analysis Division, DST Group, 2018).
3. Brian M. Ducote, “Challenging the Application of PMESII-PT in a Complex Environment” (School of Advanced Military Studies, United States Army Command and General Staff College, Fort Leavenworth, Kansas, 2010), 2-5, <https://apps.dtic.mil/dtic/tr/fulltext/u2/a523040.pdf>.
4. The literature on ‘emergence’ in complex systems is enormous for a good introduction see Harold J. Morowitz, *The Emergence of Everything: How the World Became Complex* (Oxford University Press, USA, 2002); John H. Holland, *Emergence: From Chaos to Order* (Oxford University Press, 2000); Lars-Erik Cederman, *Emergent Actors in World Politics: How States and Nations Develop and Dissolve* (Princeton University Press, 1997); Ducote’s primary influence is Jamshid Gharajedaghi, *Systems Thinking: Managing Chaos and Complexity: A Platform for Designing Business Architecture* (Butterworth-Heinemann, 2006).
5. Ducote, “Challenging the Application of PMESII-PT in a Complex Environment,” 6.
6. Zachery Brown, “Librarians of Babel: Intelligence’s Three Big Problems in the Information Age,” Real Clear Defense, December 5, 2018, https://www.realcleardefense.com/articles/2018/12/05/librarians_of_babel_intelligences_three_big_problems_in_the_information_age_114003.html; Zachery Brown, “What Would You Say You Do Here? Redefining the Role of Intelligence in the Information Age,” War on the Rocks, December 5, 2018, <https://warontherocks.com/2018/12/what-would-you-say-you-do-here-redefining-the-role-of-intelligence-in-the-information-age/>.
7. Sean T. Lawson, *Nonlinear Science and Warfare: Chaos, Complexity and the U.S. Military in the Information Age* (Routledge, 2013).
8. US Army, FM 3-13 (FM 100-6), *Information Operations: Doctrine, Tactics, Techniques, and Procedures, November 2003* (CreateSpace Independent Publishing Platform, 2012).
9. ANDREW S. ERICKSON, “America’s Security Role in the South China Sea,” *Naval War College Review* 69, no. 1 (2016): 7-21; Peter Dutton, Andrew S. Erickson, and Ryan Martinson, “China’s Near Seas Combat Capabilities” (China Maritime Study, Number 11) (DTIC Document, 2014), <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA612569>.
10. Nathan Freier et al., “Outplayed: Regaining Strategic Initiative in the Gray Zone” (Carlisle, PA: Army War College, 2016), <http://www.dtic.mil/docs/citations/AD1013807>; Douglas Lovelace, *Hybrid Warfare and the Gray Zone Threat* (Oxford: Oxford University Press, 2016).
11. Liang Qiao and Xiangsui Wang, *Unrestricted Warfare: China’s Master Plan to Destroy America* (NewsMax Media, Inc., 2002); M. Taylor Fravel, “China’s Strategy in the South China Sea,” *Contemporary Southeast Asia* 33, no. 3 (December 2011): 292-319; M. Taylor Fravel, “Power Shifts and Escalation: Explaining China’s Use of Force in Territorial Disputes,” *International Security* 32, no. 3 (January 1, 2008): 44-83, <https://doi.org/10.1162/isec.2008.32.3.44>; M. Taylor Fravel, “Regime Insecurity and International Cooperation: Explaining China’s Compromises in Territorial Disputes,” *International Security* 30, no. 2 (2005): 46-83.
12. 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>; 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/>.
13. Katherine Manstead and Eric Rosenbach, “The Geopolitics of Information,” Belfer Center for Science and International Affairs, May 28, 2019, <https://www.belfercenter.org/publication/geopolitics-information>; Katherine Manstead, “The Revenge of Geography in Cyberspace,” *The Strategy Bridge*, June 4, 2019, <https://thestategybridge.org/the-bridge/2019/6/4/the-revenge-of-geography-in-cyberspace>.
14. 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/>.
15. Shima D. Keene, “Silent Partners: Organized Crime, Irregular Groups, and Nation-States” (Strategic Studies Institute, US Army War College, October 23, 2018), <https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1392>.

NOTES

16. Barry R. Posen, "Command of the Commons: The Military Foundation of US Hegemony," *International Security* 28, no. 1 (2003): 5-46.
17. Alicia Wanless and Michael Berk, "Participatory Propaganda: The Engagement of Audiences in the Spread of Persuasive Communications," ResearchGate, accessed February 6, 2019, https://www.researchgate.net/publication/329281610_Participatory_Propaganda_The_Engagement_of_Audiences_in_the_Spread_of_Persuasive_Communications; Zac Rogers, Emily Bienvenue, and Maryanne Kelton, "The New Age of Propaganda: Understanding Influence Operations in the Digital Age," *War on the Rocks*, May 1, 2019, <https://warontherocks.com/2019/05/the-new-age-of-propaganda-understanding-influence-operations-in-the-digital-age/>.
18. Timothy Thomas, "Russia's 21st Century Information War: Working to Undermine and Destabilize Populations," *Defence Strategic Communications* 1, no. 1 (2015): 11-24; Timothy L. Thomas, *Decoding The Virtual Dragon Critical Evolutions In The Science And Philosophy Of China's Information Operations And Military Strategy The Art Of War And IW* (Foreign Military Studies Office, 2007).
19. "SMA White Paper: What Do Others Think and How Do We Know What They Are Thinking?" A Strategic Multilayer Assessment Periodic Publication (DoD, Joint Chiefs of Staff, March 2018), http://nsiteam.com/social/wp-content/uploads/2018/03/White-Paper_What-Do-Others-Think_March2018_FINAL.pdf.
20. Department of the Army, "FM 100-6 Information Operations" (Washington D.C., Office of the Chief of Staff of the Army, 1996), 100.
21. Jonathan Zittrain, "The Hidden Costs of Automated Thinking," *The New Yorker*, July 23, 2019, <https://www.newyorker.com/tech/annals-of-technology/the-hidden-costs-of-automated-thinking>; D. Sculley et al., "Machine Learning: The High Interest Credit Card of Technical Debt," in *SE4ML: Software Engineering for Machine Learning* (NIPS 2014 Workshop), 2014, <https://ai.google/research/pubs/pub43146>.
22. Charles Kriel, "Fake News, Fake Wars, Fake Worlds," *Defence Strategic Communications* 3 (2017): 171-190.
23. Bryan Sparling, "Information Theory as a Foundation for Military Operations in the 21st Century" (School of Advanced Military Studies, United States Army Command and General Staff College, Fort Leavenworth, Kansas, 2002), <https://apps.dtic.mil/dtic/tr/fulltext/u2/a403845.pdf>.
24. Carl H. Builder, "The American Military Enterprise in the Information Age," in *Strategic Appraisal: The Changing Role of Information in Warfare* (RAND Corporation, 1999), https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1016/MR1016.chap2.pdf.
25. Lawson, *Nonlinear Science and Warfare*.
26. Sparling, "Information Theory as a Foundation for Military Operations in the 21st Century," 2002, iii.
27. Sparling, 45.
28. Joint Chiefs of Staff, "Joint Concept for Operating in the Information Environment (JCOIE)" (Department of Defense, July 25, 2018), 12-13, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf.
29. 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/>.
30. Peter J. Katzenstein and Lucia A. Seybert, "Protean Power and Uncertainty: Exploring the Unexpected in World Politics," *International Studies Quarterly* 62, no. 1 (March 1, 2018): 80-93, <https://doi.org/10.1093/isq/sqx092>.
31. 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/>.
32. Information fratricide is defined as "the result of employing information operations elements in a way that causes effects in the information environment that impede the conduct of friendly operations or adversely affect friendly forces, U.S. Army, *FM 3-13 (FM 100-6) Information Operations*.
33. Charles Cleveland, Benjamin M. Jensen, and Susan Bryant, *Military Strategy for the 21st Century: People, Connectivity, and Influence* (Cambria Press, 2018).
34. Bill Roche, "Summit Helps Chart Way Ahead for Maneuver in Information Environment," www.army.mil, August 7, 2019, https://www.army.mil/article/225430/summit_helps_chart_way_ahead_for_maneuver_in_information_environment.
35. Roche.

NOTES

36. Glenn Greenwald, "How Covert Agents Infiltrate the Internet to Manipulate, Deceive, and Destroy Reputations," *The Intercept* (blog), February 24, 2014, <https://theintercept.com/2014/02/24/jtrig-manipulation/>; Fred Adkins and Shawn Hibbard, "The Coming Automation of Propaganda," *War on the Rocks*, August 6, 2019, <https://warontherocks.com/2019/08/the-coming-automation-of-propaganda/>.
37. Luciano Floridi, *The Fourth Revolution: How the Infosphere Is Reshaping Human Reality* (Oxford University Press, 2014); Seb Franklin, *Control: Digitality as Cultural Logic* (MIT Press, 2015); David Golumbia, *The Cultural Logic of Computation* (Harvard University Press, 2009); D. McCarthy, *Power, Information Technology, and International Relations Theory: The Power and Politics of US Foreign Policy and the Internet* (Springer, 2015); Duncan J. Watts, *Six Degrees: The Science of a Connected Age* (Random House, 2004).
38. Benjamin H. Bratton, *The Stack: On Software and Sovereignty* (MIT Press, 2016).
39. Ian Hodder, *Entangled: An Archaeology of the Relationships Between Humans and Things* (John Wiley & Sons, 2012); Langdon Winner, *The Whale and the Reactor: A Search for Limits in an Age of High Technology* (University of Chicago Press, 2010); David Livingstone, *Transhumanism: The History of a Dangerous Idea* (David Livingstone, 2015).
40. Bruno Latour, "Technology Is Society Made Durable," *The Sociological Review* 38, no. 1, suppl (May 1, 1990): 103-31, <https://doi.org/10.1111/j.1467-954X.1990.tb03350.x>; Bruno Latour, "How to Write the Prince for Machines as Well as for Machinations," in *Technology and Social Process* (Edinburgh University Press, 1988).
41. George Dyson, *Turing's Cathedral: The Origins of the Digital Universe* (Penguin UK, 2012); George Dyson, "Childhood's End," *Edge* (blog), January 1, 2019, https://www.edge.org/conversation/george_dyson-childhoods-end.
42. Popularized from 2010 onwards in the discourse on Air Sea Battle; see Jan Van Tol et al., "AirSea Battle: A Point-of-Departure Operational Concept" (Washington, D.C.: Center for Strategic and Budgetary Assessments, May 2010), <http://www.csbaonline.org/publications/2010/05/airsea-battle-concept/>; Andrew F. Krepinevich, "Why AirSea Battle?" (Washington: Center for Strategic and Budgetary Assessments, February 2010), <http://www.csbaonline.org/publications/2010/02/why-airsea-battle/>; Andrew F. Krepinevich, "The Future of U.S. Defense Strategy and the Japan-U.S. Alliance" (June 23, 2015), <http://csbaonline.org/2015/06/23/the-future-of-u-s-defense-strategy-and-the-japan-u-s-alliance/>.
43. P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar What Everyone Needs to Know* (New York: Oxford University Press, 2014).
44. Paul E. Ceruzzi, *Internet Alley: High Technology in Tysons Corner, 1945-2005* (MIT Press, 2008).
45. Sarah Price, "Loudoun, Virginia's Data Center Alley: Computing Power of 10 Million Servers at Plug-and-Play Price," *Loudoun County Economic Development, VA* (blog), January 4, 2019, <https://biz.loudoun.gov/2019/01/04/loudoun-virginias-data-center-alley-computing-power-of-10-million-servers-at-plug-and-play-price/>.
46. "The World's Most Valuable Resource Is No Longer Oil, but Data," *The Economist*, May 6, 2017, <https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource>; Ioanna D. Constantiou and Jannis Kallinikos, "New Games, New Rules: Big Data and the Changing Context of Strategy," *Journal of Information Technology* 30, no. 1 (March 1, 2015): 44-57, <https://doi.org/10.1057/jit.2014.17>; Zac Rogers, "Data Is Not the New Oil; Data Is the New Sea," *The Fox and the Grapes* (blog), May 17, 2017, <https://thefoxandthegrapesblog.wordpress.com/2017/05/17/data-is-not-the-new-oil-data-is-the-new-sea/>.
47. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2019).
48. Andrew Keen, *Digital Vertigo: How Today's Online Social Revolution Is Dividing, Diminishing, and Disorienting Us* (St. Martin's Press, 2012).
49. Douglas Rushkoff, *Team Human* (New York: W.W. Norton & Company, 2019).
50. Martin Moore, *Democracy Hacked: Political Turmoil and Information Warfare in the Digital Age* (Oneworld Publications, 2019).
51. Peter Layton, "Social Mobilisation in a Contested Environment," *The Strategist*, August 5, 2019, <https://www.aspistrategist.org.au/social-mobilisation-in-a-contested-environment/>.

NOTES

52. Christopher Sims, “The Military and the Internet: Will War as We Know It Become Outmoded?” *Modern War Institute* (blog), July 18, 2019, <https://mwi.usma.edu/military-internet-will-war-know-become-outmoded/>; Sebastien Bay and Nora Biteniece, “The Current Digital Arena and Its Risks to Serving Military Personnel,” Responding to Cognitive Security Challenges (Latvia: NATO STRATCOM COE, January 2019), <https://stratcomcoe.org/current-digital-arena-and-its-risks-serving-military-personnel>.
53. Rob Ackland and Zac Rogers, “Mapping Australia’s Blockchain Ecosystem: Insights from Digital Trace Data” (April 18, 2019).
54. Julie A. Jacko, *Human Computer Interaction Handbook: Fundamentals, Evolving Technologies, and Emerging Applications*, Third Edition (CRC Press, 2012); B.J. Fogg, *Persuasive Technology: Using Computers to Change What We Think and Do* (Morgan Kaufmann, 2003); Woodrow Hartzog, *Privacy’s Blueprint: The Battle to Control the Design of New Technologies* (Cambridge: Harvard University Press, 2018).
55. National Research Council et al., *Emerging Cognitive Neuroscience and Related Technologies* (National Academies Press, 2008); 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).
56. Robert Rubel, “Talking about Sea Control,” *Naval War College Review* 63, no. 4 (2010), <https://digital-commons.usnwc.edu/nwc-review/vol63/iss4/6>.
57. Randy Huis, “Proliferation of Precision Strike: Issues for Congress” (Congressional Research Service, May 14, 2012), <http://fas.org/sgp/crs/nuke/R42539.pdf>.
58. Lindsey A. O’Rourke, *Covert Regime Change: America’s Secret Cold War* (Ithaca, NY: Cornell University Press, 2018); Austin Carson, *Secret Wars: Covert Conflict in International Politics* (Princeton, NJ : Princeton University Press, 2018).
59. George R. Lucas, Jr., *Ethics and Military Strategy in the 21st Century: Moving Beyond Clausewitz* (Routledge, 2019).
60. Katie Collins, “Ukraine Blackout Is a Cyberattack Milestone,” CNET, January 5, 2016, <https://www.cnet.com/news/cyberattack-causes-widespread-power-blackout-in-ukraine/>; Youssa Khalil, “With the Internet Blackout in Sudan, Knowledge Is Power,” The Washington Institute, June 25, 2019, <https://www.washingtoninstitute.org/policy-analysis/view/with-the-internet-blackout-in-sudan-knowledge-is-power>; Niha Masih, “‘I’m Just Helpless’: Concern about Kashmir Mounts as Communication Blackout Continues,” *The Washington Post*, August 6, 2019, sec. Asia & Pacific, https://www.washingtonpost.com/world/internet-mobile-blackout-shuts-down-communication-with-kashmir/2019/08/06/346d5150-b7c4-11e9-8e83-4e6687e99814_story.html.
61. Ian Langford, “Accelerated Warfare,” February 27, 2019, <https://www.army.gov.au/accelerated-warfare-0>.
62. Bryan Sparling, “Information Theory as a Foundation for Military Operations in the 21st Century” (School of Advanced Military Studies, United States Army Command and General Staff College, Fort Leavenworth, Kansas, 2002), 51, <https://apps.dtic.mil/dtic/tr/fulltext/u2/a403845.pdf>.
63. Niall McCarthy, “The Institutions Americans Trust Most And Least In 2018,” *Forbes*, June 29, 2018, <https://www.forbes.com/sites/niallmccarthy/2018/06/29/the-institutions-americans-trust-most-and-least-in-2018-infographic/>.
64. Rogers, “158. In the Cognitive War – The Weapon Is You!”

Risks to the Mission Partner Environment: Adversarial Access to Host Nation Network Infrastructure

Captain Kyle Sullivan

ABSTRACT

NATO's ability to communicate and win in the next conflict is based on the idea of Federated Mission Networking (FMN). The US initiative for the FMN is the Mission Partner Environment (MPE). This framework is built around the use of host nation network infrastructure. Recently, adversarial nations have been investing and developing host nation network infrastructure for NATO allies and partners. China, through companies such as Huawei, is leading the development of next-generation networking technologies. Russia has shown in recent conflicts that it will target a nation's network infrastructure to achieve its military goals. Russian political strategy is to expand its control over the strategic industries of countries in its sphere of influence. National network infrastructure will be considered strategic in the next conflict. Adversarial access to a host nation's network infrastructure threatens the MPE and NATO's ability to operate as a unified alliance. NATO must develop a strategy for a unified response by its member nations to protect their network infrastructures against unsecured network equipment of adversarial countries. NATO should also invest in options to provide secure communications for future mission partners which may have already sold control of their national network infrastructure to an adversary.

INTRODUCTION

At the 2014 Wales Summit, the North Atlantic Treaty Organization (NATO) passed the Connected Forces Initiative (CFI). This initiative set forth the goal of creating an interoperable force capable of operating alongside mission partners in any environment. The CFI implemented the idea of Federated Mission Networking (FMN), which provides the ability for ally and partner forces to communicate, train, and

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



Kyle Sullivan is currently a Captain in the U.S. Army Signal Corps and a graduate of the Joint Command, Control, Communications, Computers, and Intelligence/Cyber Staff and Operations Course (JC4/CSOC) at the National Defense University. He has a B.S. in Computer Science as well as an M.S. in Cybersecurity from the University of Delaware. In his civilian life, he has worked as a software engineer at the Army's Software Engineering Center in Aberdeen Proving Grounds, Maryland, and holds professional certifications in cybersecurity. In the military, he has served in a variety of joint assignments where he implemented Mission Partner Environment communications alongside NATO allies in countries such as Croatia, Bosnia, Bulgaria, Hungary, Iraq, Italy, Romania, and Slovenia.

operate together.^[1] The U.S.-based initiative for the FMN is called the Mission Partner Environment (MPE). The MPE is a network that enables information sharing by NATO allies and mission partners and creates unity of effort for mission forces down to the tactical level. In essence, the MPE is how NATO will perform Command, Control, Communications, Computers, and Intelligence (C4I) with its mission partners during future operations. A joint publication on Joint Communication Systems outlines how “the MPE is established using mission partner communications network infrastructure.”^[2] The MPE framework is therefore designed around the use of host nation network infrastructure for its success. However, in recent years adversarial nations have been investing in network infrastructure within NATO and partner countries.^[3] Adversarial access to host nation network infrastructure poses several cybersecurity risks that threaten the MPE. These risks can degrade or deny NATO’s ability to perform C4I during operations, which would severely impact the ability of the alliance to accomplish its mission. NATO and its partners must mitigate the cybersecurity risks to the Mission Partner Environment by working with host nations to reduce adversarial access to host nation network infrastructure.

China: The Red Team Dragon

As far back as the 1980s, the government of China identified telecommunications infrastructure to be strategically important and a source of technological strength.^[4] Today, this strategic goal is still being pursued by China as made evident by the rise of Chinese companies which are investing in network infrastructure around the world. In recent months, Chinese-backed companies such as ZTE and Huawei have increased their efforts to expand in Europe, especially in the emerging 5G technology field.^[5] Pressure by Chinese companies to build network infrastructure in Europe has gained enough momentum that it now “seems inevitable that [they] will build large portions of [the]

5G infrastructure – including for some of the US’ closest allies.”^[6] As a result, the future of European network infrastructure is concerning given the influence of Chinese-based companies. This poses a risk to the MPE framework because the network infrastructure of European countries, many of which are NATO allies and partners, will be influenced and tied to China, which is a non-NATO nation.

While China is not a formally recognized adversary, the 2019 NATO Summit announced that “China has security implications for all allies,”^[7] insinuating an adversarial-style role. The framework for MPE was designed with the use of host nation infrastructure in mind, but underneath is an inherent assumption that the host nation has control of the network. If a host nation loses control of its network infrastructure, it will compromise its ability to operate within the MPE. If a nation-state actor, such as China, can leverage access or control over a nation’s network infrastructure, it could divide or isolate a NATO ally or partner, reducing the effectiveness of the alliance. In the worst-case scenario, an adversary could deny a NATO ally or partner access to the MPE. This would prevent that nation from information-sharing abilities and prevent it from being able to operate alongside mission partners as a unified force, ultimately undermining interoperability.

Currently, there has been a mixed response from NATO countries to the use of Chinese network equipment in national infrastructure.^[8] Across the alliance there are differing opinions on how a nation should invest in and develop its network infrastructure. As a result, it remains unclear how secure the future backbone of the MPE will be from a meddling nation-state actor like China.

Russia: The Grey Hat Bear

Russia, a traditional adversary of NATO, has shown in recent conflicts that it is willing and able to disrupt network infrastructure of its adversaries and will leverage cyberattacks to further its goals. In the 2008 conflict with Georgia, Russia exploited Georgian communications by leveraging physical proximity to network infrastructure. This was because the national network infrastructure of Georgia ran through Russian territory, which allowed Russia access to launch cyberattacks and effectively control the host nation network.^[9] Furthermore, Russia conducted military operations to cut fiber and disrupt other infrastructure across Georgia to deny Georgia the ability to communicate and force the use of Russian-controlled network infrastructure.

These strategies were employed once again a few years later in the 2014 conflict with Ukraine over the disputed territory of Crimea. During the Crimean conflict, Russian forces showcased their cyber capabilities and conducted cyberattacks on the Ukrainian power grid, demonstrating how powerful cyber effects can be.^[10] These cyberattacks were not only aimed at Ukraine but also against various European organizations including NATO. At the start of the conflict, “various NATO websites were hit by denial-of-service attacks, and NATO servers were infected by the same malware that infected Ukrainian institutions.”^[11] These attacks could have

been made as an effort to stop any NATO involvement during the conflict. During the Crimean annexation, Russia demonstrated the strategic advantage of targeting host nation network infrastructure. In the midst of the conflict, Russian forces conducted a military raid on Ukrainian network infrastructure during which they cut off Crimean communications and isolated them from the outside world.^[12] Had Ukraine been a NATO ally during the conflict, its ability to operate within the MPE may have been denied. As a result, a unified NATO response to the Russian aggression would have been hindered as mission partners were isolated and unable to communicate. The effects of these cyberspace attacks grant Russia a clear strategic advantage during a future conflict. Russia continues to achieve these same strategic advantages before the onset of the next conflict through its ongoing political strategy across Europe.^[13]

Russian strategy is to gain access or control of the national infrastructures in its sphere of influence, such as in the Baltics and the Balkans.^[14] This access can enable Russia to compromise a nation's network infrastructure during a conflict, either through control of power generation (e.g., disrupting the power grid) or through physical proximity to network equipment allowing for exploitation. While Russia does not exercise the same economic influence that China does with developing and exporting network technologies, Russia has used the same strategies as China in recent years in its attempts to control host nation network infrastructure.

Based on reports by the US and allied cyber intelligence agencies, Russia has been discovered using hacking techniques to exploit network infrastructure devices across nations worldwide in attempts to seize key cyber terrain.^[15] Once network devices are exploited, Russian hackers can remain in hiding and wait for a strategic opportunity to launch cyberattacks. These network device exploits conducted by Russian state-sponsored cyber actors achieve the same ultimate goal as pursued by Chinese companies such as Huawei, etc., to access and control a nation's network infrastructure. Russia has shown in past conflicts that it will target network infrastructure and, based on its current strategy, will continue to do so again in the future.

This threat is further amplified by closer relations between China and Russia. With the implementation of China's New Silk Road initiative in 2015, network infrastructure has been built directly between Russia and China to shield the two countries from US and Western intelligence agencies and further align the two nations.^[16] With this in mind, it is not difficult to imagine that, at the start of a conflict with NATO, an adversary such as Russia would be quick to target and disrupt network infrastructure. In doing so, it would deny the ability of an invaded nation to communicate and operate on the MPE, thus preventing a unified NATO response.

Threats to Cyberspace: The Fifth Domain

As the physical world evolves into the cyberspace domain, it is increasingly true that "network equipment is now integral to the critical infrastructure of any country."^[17] From a technological perspective, "the equipment vendors of these network infrastructures pose a real threat to national security."^[18] If an adversary controls the network between two parties, it allows for a variety of attacks such as the Man-In-The-Middle attack (MITM).^[19] Moreover,

while cryptography technologies may protect the confidentiality of communications, MITM attacks can still allow for a variety of other malicious actions such as a denial-of-service attack.^[20] Additionally, the strength of cryptography is always being tested, in which new methods such as “side channel attacks”^[21] are emerging and prove to be extremely difficult to defend against.^[22] With control over network infrastructure, an adversary would have access to critical information that could be leveraged for malicious means. With access to network base stations, which are primarily being installed by Huawei, an adversary would “possess a complete overview of where all mobile equipment is located, and thus, where all users are located.”^[23] This access could facilitate the leakage of sensitive information such as troop movements, which would provide vital military intelligence to an adversary. In addition to intelligence gathering, an adversary could “choose to turn off parts of the country’s infrastructure or modify the infrastructure so it only works for their armed forces.”^[24] There are endless possibilities that an adversary could pursue if it controls network infrastructure.

All these threats are underlined by the fact that it is “way beyond feasible”^[25] to analyze network equipment completely and verify it is secure. For a nation to trust the equipment in their network infrastructure fully, “the producer must remain trustworthy throughout the product's lifetime.”^[26] This means that using third-party equipment will always pose a risk to a nation’s network infrastructure. These cybersecurity risks threaten the MPE and stand to undermine the interoperability of NATO.

Recommendations: An Interoperable NATO Response

The strategic importance of network infrastructure cannot be understated. Just as a nation protects its critical military equipment, so too must a nation protect its network infrastructure. NATO must make clear to all members that threats posed to network infrastructure not only impact the host nation itself but threaten the effectiveness of the alliance. NATO can use its political influence with member nations to ensure a unified response to using third-party network equipment such as that offered by Huawei. This can be accomplished through normal diplomatic means or by expanding the CFI at a subsequent summit to address using third-party equipment. At the very least, as NATO nations develop their mission networks, they need to identify critical segments of their network infrastructure and ensure only trustworthy equipment is being installed. While this may be possible in NATO countries, there will still be challenges with other mission partners which may not even be identified until a mission is already underway.^[27] By the time a mission partner needs to operate within the MPE, its network infrastructure may already be controlled by an adversary. NATO must invest in flexible communications options that it can deploy to provide a secure networking backbone and enable the MPE in situations where the network infrastructure of a host nation is compromised. These flexible options could take the form of tactical mobile networking assets which are sourced from trustworthy producers and stockpiled before the next conflict.

CONCLUSION

NATO's Connected Forces Initiative outlines how it will use host nation network infrastructure to communicate and win in future conflicts with US allies and partners. Adversarial nations are vying for control and influence over strategic national network infrastructures. It is these network infrastructures that will be the backbone for the Mission Partner Environment and set the stage for future battlefields. NATO nations will have to align their political goals for national development with their strategic goals of protecting network infrastructure to ensure NATO remains an interoperable alliance. NATO can do this by enacting initiatives for member nations to identify strategic network infrastructure and develop them only by using trustworthy suppliers. For mission partners, NATO can stockpile secure network equipment to be deployed for use in contested network environments. Adversaries have demonstrated that they have the ability to access our networks, possess the technical skills, and that they lack the legal safeguards^[28] to launch cyberattacks against NATO allies and partners. NATO must continue to defend strategic cyberspace terrain to ensure its greatest strength is preserved—interoperability. Through interoperability, members can act together coherently, effectively, and efficiently as an alliance, ensuring NATO will continue to guarantee the freedom and security of its members around the world.🇺🇸

DISCLAIMER

The views expressed in this work are those of the author 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. "FEDERATED MISSION NETWORKING," NATO, accessed March 15, 2020, <https://www.act.nato.int/activities/fmn>.
2. U.S. Department of Defense, "Joint Communication Systems," Joint Publication 6-0, October 4, 2019.
3. The most prevalent example is China with its company Huawei; source: Lawrence Norman "Huawei Faces Deepening Scrutiny in Europe," *The Wall Street Journal*, Dow Jones & Company, January 31, 2019, <https://www.wsj.com/articles/huawei-faces-deepening-scrutiny-in-europe-11548930489>.
4. Deborah Brautigam, *The Dragon's Gift: The Real Story of China in Africa* (Oxford: Oxford University Press, 2011), 74.
5. 5G technology refers to the fifth generation of mobile networks which, in addition to faster communication speeds, intends to be the connectivity means of choice for various industries. These include automotive, health, public safety, armed forces, manufacturing, smart cities, and home automation.
6. Joseph Marks, "The Cybersecurity 202: The U.S. Is Going after Huawei, but It Isn't Changing Allies' Minds," *The Washington Post*, February 14, 2020.
7. Christopher Woody, "NATO Is Finally Talking about China, and There Are 3 Big Problems It Has to Address," *Business Insider*, December 12, 2019, <https://www.businessinsider.de/international/china-poses-3-problems-in-europe-for-nato-2019-12/?r=US&IR=T>.
8. Responses range from the United States outright banning Chinese companies such as Huawei, to Germany, UK, and France moving cautiously and taking a risk mitigation approach but still conducting business with Huawei. Some countries such as Italy, Austria, Poland, Estonia, and Lithuania, are undecided, while other NATO countries such as Spain and Slovakia are openly accepting Chinese investment and currently moving forward with Huawei equipment.
9. R.J. Deibert, R. Rohozinski, and M. Crete-Nishihata, Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war, *Security Dialogue*, 2012, 43(1), 3-24; doi:10.1177/0967010611431079.
10. Marie Baezner and Patrice Robin, "Cyber and Information Warfare in the Ukrainian Conflict," Center for Security Studies (CSS), October 2018, https://www.researchgate.net/publication/322364443_Cyber_and_Information_warfare_in_the_Ukrainian_conflict.
11. Ibid.
12. Tony Martin-Vegue, "Are We Witnessing a Cyber War between Russia and Ukraine? Don't Blink You Might Miss It," *CSO Online*, April 24, 2015, <https://www.csoonline.com/article/2913743/are-we-witnessing-a-cyber-war-between-russia-and-ukraine-dont-blink-you-might-miss-it.html>.
13. Russia implements its strategy via threats to gas supplies and acquiring energy or power assets across Europe. Sometimes Russian state-owned proxy companies acquire entire retail chains for energy products.
14. Stefan Ralchev, "Energy in the Western Balkans: A Strategic Overview," *Institute for Regional and International Studies*, August 2012, https://www.iris-bg.org/fls/Energy_in_the_Western_Balkans_Overview__Aug12.pdf.
15. Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices, April 2018, retrieved August 2, 2020, https://us-cert.cisa.gov/ncas/alerts/TA18-106A?utm_source=newsletter.
16. N. Rolland, August 15, 2019, China's Belt and Road Initiative: Five Years Later, retrieved March 20, 2020, from <https://www.nbr.org/publication/chinas-belt-and-road-initiative-five-years-later/>.
17. Olav Lysne, Ahmed Elmokashfi, Niels Nagelhus Schia, Lars Gjesvik, and Karsten Friis, "Critical Communication Infrastructures and Huawei," TPRC 2019, July 2019, <https://doi.org/10.2139/ssrn.3426222>.
18. Ibid.
19. Man-In-The-Middle (MITM) is a kind of attack in which a malicious third party takes control of a communication channel. The attacker can intercept, modify, change, or replace target victims' communication traffic.
20. Mauro Conti, Nikola Dragoni, and Viktor Lesyk, "A Survey of Man In The Middle Attacks," *IEEE Communications Surveys & Tutorials* 18, no. 3, March 2016, <https://doi.org/10.1109/COMST.2016.2548426>.
21. Side Channel Attacks pose a real and serious threat to user privacy as they present a way to defeat encryption using information leaking in a side-channel. Source: Chen, Shuo, Rui Wang, XiaoFeng Wang, and Kehuan Zhang, "Side-Channel Leaks in Web Applications: A Reality Today, a Challenge Tomorrow," Proceedings of the IEEE Symposium on Security and Privacy (Oakland), May 2010, <https://www.microsoft.com/en-us/research/publication/side-channel-leaks-in-web-applications-a-reality-today-a-challenge-tomorrow/>.

NOTES

22. Eyal Ronen, Robert Gillham, Daniel Genkin, Adi Shamir, David Wong, and Yuval Yarom, “The 9 Lives of Bleichenbachers CAT: New Cache Attacks on TLS Implementations,” 2019 IEEE Symposium on Security and Privacy (SP), 2019, <https://doi.org/10.1109/sp.2019.00062>.
23. Olav Lysne, Ahmed Elmokashfi, Niels Nagelhus Schia, Lars Gjesvik, and Karsten Friis, “Critical Communication Infrastructures and Huawei,” TPRC 2019, July 2019, <https://doi.org/10.2139/ssrn.3426222>.
24. Ibid.
25. Ibid.
26. Ibid.
27. T. Buckman, “NATO Network Enabled Capability Feasibility Study,” NATO Consultation, Command and Control Agency, October 2005, http://www.dodccrp.org/files/nnec_fs_executive_summary_2.0_nu.pdf.
28. Murray Scot Tanner, “Beijing’s New National Intelligence Law: From Defense to Offense,” Lawfare Blog, Lawfare Institute, July 20, 2017, <https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense>.

THE CYBER DEFENSE REVIEW

◆ RESEARCH NOTES ◆

China Arctic Cyber Espionage

Emilio Iasiello

ABSTRACT

China is one of the most pervasive actors conducting global cyber espionage, activities that have resulted in two indictments by the U.S. Department of Justice. One thing is clear – if a target or subject area is in China’s strategic interest, it is likely that some level of cyber espionage is being levied against that target, as well as any organization involved in that subject. While reporting by the many countries bordering the Arctic on Chinese cyber-espionage has been limited, given China’s high interest in the Arctic, and its espionage proclivities, China’s activity may well be either undetected or under-reported.

China’s Arctic Aspirations – An Under-Reported Cyber Espionage Hot Spot?

China has vociferously promoted itself as a legitimate “Arctic State”—it included the region in its strategic planning for the 2011 Twelfth Five-Year Plan,^[1] and in a 2018 publication delineating its Arctic Policy.^[2] China further demonstrated its commitment via a series of economic opportunities to attain influence in this area of rising strategic, economic, environmental, and maritime importance. Incorporating the Arctic into its strategic documents underscores China’s elevation of this region to a national-level priority. The Arctic falls squarely within China’s long-term global leadership and economic power goals and presents an opportunity to enhance China’s presence in less-emphasized areas of the world, particularly where neither the US nor Russia have dedicated much time or attention. As it did in Africa, Beijing is resorting to its win-win playbook,^[3] enticing local states via economic engagement and financial investment in return for support for Chinese projects.



Emilio Iasiello has nearly 20 years' experience as a strategic cyber intelligence analyst, supporting U.S. Government civilian and military intelligence organizations, as well as the private sector. He has delivered cyber threat presentations to domestic and international audiences and has published extensively in such peer-reviewed journals as *Parameters*, *Foreign Policy Journal*, *Journal of Strategic Security*, *Georgetown Journal of International Affairs*, and *The Cyber Defense Review*, among others. All comments and opinions expressed are solely his own. Emilio Iasiello - iasiello@aol.com

Economic engagement clearly seems to be a primary objective, particularly in the underdeveloped Arctic region, which tracks China's approach in Africa^[4] and Latin America,^[5] with construction and infrastructure projects tied to important trade agreements. The Arctic provides China a polar component to its Belt and Road Initiative, a "transcontinental, long-term policy and investment program" focused on developing infrastructure and economic integration for countries along the historic Silk Road.^[6] Access to natural resources and establishing a maritime trade route factor into China's calculus. Indeed, Chinese investment has focused largely on energy-related efforts under the Silk Road banner. Per a 2008 U.S. Geological Survey, the Arctic retains an estimated thirteen percent of the Earth's undiscovered natural gas, and as much as ninety billion barrels of oil.^[7] China's appetite for natural resource consumption is well known, and, according to a 2019 report, China is increasing imports from resource-rich countries.^[8] Fisheries, mining, and shipping are other unexplored areas of Chinese exploitation.

China's Investment – China's Influence

China has invested heavily in nearly every Arctic country in the form of joint projects that see both partners receiving a benefit. In the case of at least two countries on the Arctic Council, Chinese investments represented a significant percentage of their annual gross domestic product, according to one 2017 report.^[9] China is prospecting for minerals in Greenland, and working with a Finnish company seeking to lay under-sea Internet cables to connect Northern Europe and Asia.^[10] Beijing's collaboration with Moscow includes a joint project to build ice-capable tanker ships to help extract from Arctic-based energy sources.^[11] China and Russia are also trying to establish a Northern Sea Route that would reduce transportation time by 40 percent compared to the Suez Canal.^[12] The magnitude of investment differs among the Arctic countries, for some the dependence on Chinese engagement is significant.

While economics is a driving force, China views the Arctic the key to its emergence as a global power. According to one think tank focusing on Arctic issues, the region offers China a place where it can exert its influence via infrastructure projects, and by extension, feed its wealth into the region.^[13] This is a necessary step for Beijing, which made its first overture in the Arctic in 1999 with expeditions, which resulted in building a research facility on Svalbard Island in 2004.^[14] Nine years later, China officially joined the Arctic Council, an intergovernmental forum promoting cooperation and coordination among Arctic states with a focus on “sustainable development and environmental protection in the Arctic.”^[15] Consisting of eight primary states (Canada, Denmark, Finland, Iceland, Norway, Russia, Sweden, and the US), China attained permanent observer status in 2013. Observer nations lack voting rights and cannot challenge the ownership of the five coastal Arctic states.^[16] Barring charter amendments, Beijing’s role is limited to discussion and recommendation only. Yet, engaging in multilateral approaches has been a favored tactic of China (witness China’s preference in establishing cyber norms of behavior^[17]), particularly when it lacks the capability to dictate a course of action among international groups. Voting countries that rely on Chinese funding help Beijing get what it wants.

Why China’s Forays into the Arctic are a Concern

Unsurprisingly, while China’s playbook has been effective in the past, it is hardly subtle or below the US radar screen and efforts to curb China’s global expansion. Beijing touts itself as a “near-Arctic state” in its 2018 Arctic Policy,^[18] signaling its intentions of being a regional player. China sought a foothold in areas like Greenland, first trying to buy an old military base in 2016,^[19] followed by then withdrawing its bid to build two airport projects on the world’s largest island.^[20] Greenland has long been of strategic military importance for the US, and any Chinese presence threatens US missile defense and space situational awareness capabilities.^[21] However, concerns about China’s attempts to expand its sphere of influence in the Arctic go beyond the US. Another permanent observer nation, Japan, as well as Denmark, Norway, and Sweden, have recognized the potential threat of China’s military presence in the Arctic.^[22]

China is no stranger to such push-back and uses various diplomatic, economic, and cultural tacks to reduce the global perceptions of its hegemonic aspirations. China’s national security objectives obviously include preserving China as a regional and national power,^[23] so ascertaining foreign governments’ positions on relevant issues is key. Cyber espionage has allowed China to bolster its traditional human intelligence-collection platform, conducting multiple remote operations against myriad global targets. Numerous cyber espionage campaigns relate to China with various attribution levels, suggesting that Chinese national state and nonstate actors may be working to meet Beijing’s intelligence needs. Indeed, China’s global cyber-espionage activities have been well documented, including official U.S. Department of Justice (DOJ) indictments of Chinese civilian, military, and government actors.^[24] These indictments implicate these individuals for supporting operations that gained unauthorized access into and stealing sensitive information from organizations in the following areas: automotive, aviation, banking, communications technology, healthcare, and oil and gas, to name a few.

Increasingly, as DOJ indictments of Chinese officials graphically reveal, the dynamic nature of the geopolitical landscape requires timely, accurate, and actionable information. Recent targeting of U.S. Presidential campaigns^[25] is but one example of probing the positions of the two presidential candidates on issues of Chinese concern. Chinese cyberspies also often hack governments in Asia on region-related issues.^[26] Also reported is the fact that China's trading partners are a victim of cyber theft by China.^[27] It is logical to presume that even where China has not yet acquired dominating influence, it could well be engaged in cyber espionage activities to gain an advantage ahead of any decisions.

Potential Targets for China's Cyber Espionage

Given the importance China places on the Arctic region, they could well be targeting the permanent membership, as well as other states with observer status. Several Council working groups set Arctic policy that could seriously affect China's long-term plans. Working groups—such as Protection of the Arctic Marine Environment (focusing on Arctic shipping, marine protected areas, and resource exploration), Arctic Monitoring and Assessment Programme (focusing on documenting maritime pollution trends, sources and pathways of pollution, and climate change trends), and Sustainable Development (which works to protect and enhance the environment, economy, social conditions and health of indigenous communities and Arctic inhabitants), all address issues largely ignored by China. China's reputation as a notorious polluter^[28] and a colonizer in Africa^[29] could well align Arctic Council members against China's initiatives, which Beijing would do well to understand sooner rather than later, so cyber espionage against key country participants, their offices, and relevant organizations would benefit China.

Cyber espionage goes on during peacetime, tension, or conflict, and its long reach in the lead up to major events such as bilateral meetings, economic fora, and the congregation of international organizations. Knowing this, stakeholders should increase their security defenses and seek to reduce the risk of data breaches. Socializing the tactics, techniques, and procedures (TTP) of Chinese cyber threat actors can also further bolster security postures. While TTPs evolve, China's cyber espionage campaigns often execute tried-and-true methods such as spear phishing, watering hole attacks, and use of "zero-day" exploits.

Open-source reporting focused on cyber threats to the countries in the Arctic region is quite limited. A 2015 report by a computer security vendor highlighted the targeting of several Nordic country industries by suspected Chinese and Russian attackers,^[30] China's denials notwithstanding.^[31] Whether these operations were motivated by China's Arctic interests is unclear, but the report does suggest that China's interest in the region and certain Arctic Council monitored industries. Russia has long been the primary threat to Nordic countries, but in 2019 the president of the Nordic Council, the formal cooperation among the Nordic

countries, cited both Russia (militarily) and China (economically) as major threats to the region.^[32] It is no secret that China's economic interests are likely catalysts for Beijing's suspected cyber espionage activities.

Russia's perception of China in the Arctic is worth noting. An Arctic Council member, Russia has some joint projects underway with China, but this alliance likely is more economic in nature, given Moscow's likely concerns with China's military presence in the region.^[33] This could put the two collaborators at odds, and invite Beijing's cyber attention, despite a 2015 China-Russia agreement not to hack each other or use technology as a destabilizing medium (among other provisions).^[34] Given that governments inevitably operate so as to preserve all vital national security objectives, the promises exchanged in this pact at best are of dubious substance, to say nothing of enforceability. Cyber espionage will persist so long as such spying does not damage information integrity or destroy system operations of targeted networks.

CONCLUSION

China's vast and pervasive cyber espionage apparatus has a proven ability to conduct large-scale operations. However, it has also executed more stealthy campaigns, using sophisticated TTPs and front companies to obfuscate their identities.^[35] Beijing's publication of an Arctic policy underscores that the Arctic is of high national interest. As it seeks to implement the Polar Silk Road and other natural resource endeavors as part of its economic plan, understanding Nordic countries' positions on issues that could adversely impact Chinese aspirations will be important for Beijing. Knowing this beforehand will help China develop strategies to counter oppositionist viewpoints and political/economic tactics designed to persuade detractors to change, or at least soften, their positions.

What is clear is that China's "peaceful rise" has been tarnished via a series of Chinese missteps that range from its hand in authoritarian rule, its questionable track record on humanitarian issues, its rampant global intellectual property theft, to its suspicious attempt to be an instrumental developer of global 5G network. Now, as the world grapples with COVID-19, China's reputation has further been sullied, as it has been accused of being less than forthcoming and transparent regarding the virus. China combats such bad press via a public-facing propaganda and information campaign while leveraging cyber espionage in the background to obtain the information it needs.

Tactics used in the past, especially in underdeveloped regions like Africa, may not work in the Arctic. As such, China will have to develop a different approach that will require better understanding of regional leaders, what they want, and what they hope to accomplish. And that may require getting inside their heads, the type of information that cyber espionage is adept at collecting.♥

NOTES

1. Heljar Havnes and Johan Martin Saland, "The Increasing Security Focus in China's Arctic Policy," The Arctic Institute, July 16, 2019, <https://www.thearcticinstitute.org/increasing-security-focus-china-arctic-policy/>.
2. "China's Arctic Policy," State Council Information Office of the People's Republic of China, January 26, 2018, http://english.www.gov.cn/archive/white_paper/2018/01/26/content_281476026660336.htm.
3. Nick Van Mead, "China in Africa: Win-Win Development or a New Colonialism?" *The Guardian*, July 31, 2018, <https://www.theguardian.com/cities/2018/jul/31/china-in-africa-win-win-development-or-a-new-colonialism>.
4. Wade Shepard, "What China Is Really Up to in Africa?" *Forbes*, October 3, 2019, <https://www.forbes.com/sites/wadeshepard/2019/10/03/what-china-is-really-up-to-in-africa/#1824e3f05930>.
5. Miquel Vila Moreno, "The Geopolitics of China in Latin America in Donald Trump's Era," *IsagItalia*, April 30, 2017, https://isagitalia.org/the-geopolitics-of-china-in-latina-america-in-donald-trump-era/wp_8846263/.
6. "Belt and Road Initiative," <https://www.beltroad-initiative.com/belt-and-road/>.
7. Thomas E. Moore and Janet K. Pitman, "Geology and Assessment of Undiscovered Oil and Gas Resources of the Eurasia Basin Province, 2008," USGS Publication Warehouse, <https://pubs.er.usgs.gov/publication/pp1824DD>.
8. "China and the World," McKinsey Global Institute, July 2019, <https://www.mckinsey.com/-/media/mckinsey/featured%20insights/china/china%20and%20the%20world%20inside%20the%20dynamics%20of%20a%20changing%20relationship/mgi-china-and-the-world-full-report-june-2019-vf.ashx>.
9. Mark E. Rosen and Cara B. Thuringer, "Unconstrained Direct Foreign Investment: An Emerging Challenge to Arctic Security," November 2017, https://www.cna.org/CNA_files/PDF/COP-2017-U-015944-1Rev.pdf. *CNA Analysis and Solutions*.
10. Somini Sengupta and Steven Lee Myers, "Latest Arena for China's Growling Global Ambitions: The Arctic," *The New York Times*, May 24, 2019, <https://www.nytimes.com/2019/05/24/climate/china-arctic.html>.
11. Marisa R. Lino, "Understanding China's Arctic Activities," *IJSS*, February 25, 2020, <https://www.ijss.org/blogs/analysis/2020/02/china-arctic#:~:text=The%20People's%20Republic%20of%20China,image%20as%20a%20major%20power>.
12. Swee Lean and Collin Koh, "China's Strategic Interest in the Arctic Goes Beyond Economics," *Defense News*, May 12, 2020, <https://www.defensenews.com/opinion/commentary/2020/05/11/chinas-strategic-interest-in-the-arctic-goes-beyond-economics/>.
13. Yun Sun, "Defining the Chinese Threat in the Arctic," The Arctic Institute, April 7, 2020, <https://www.thearcticinstitute.org/defining-the-chinese-threat-in-the-arctic/>.
14. "China Opens First Research Station in Arctic Area," Embassy of the People's Republic of China in the United States, July 28, 2004, <http://www.china-embassy.org/eng/gyzg/t144196.htm>.
15. The Arctic Council, <https://arctic-council.org/en/about/>.
16. Matt McGrath, "China Joins Arctic Council But a Decision on the EU is Deferred," *BBC News*, May 15, 2013, <https://www.bbc.com/news/science-environment-22527822>.
17. Adam Segal, "When China Rules the Web," *Foreign Affairs*, September/October 2018, <https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web>.
18. "China's Arctic Policy," State Council Information Office of the People's Republic of China, January 26, 2018, http://english.www.gov.cn/archive/white_paper/2018/01/26/content_281476026660336.htm.
19. Marisa R. Lino, "Understanding China's Arctic Activities."
20. "China Withdraws Bid for Greenland Airport Projects: Sermitsiaq Newspaper," *Reuters*, June 4, 2019, <https://www.reuters.com/article/us-china-silkroad-greenland/china-withdraws-bid-for-greenland-airport-projects-sermitsiaq-news-paper-idUSKCNIT5191>.
21. Aaron Mehta and Valerie Insinna, "Greenland's Not for Sale, But It's Strategically Important," *Defense News*, August 16, 2019, <https://www.defensenews.com/global/europe/2019/08/16/greenlands-not-for-sale-but-it-is-strategically-important/>.
22. Heljar Havnes and Johan Martin Saland, "The Increasing Security Focus in China's Arctic Policy,".

NOTES

23. Col. [ARMY/MARINES/AIR FORCE?] Jayson M. Spade, "Information as Power: China's Cyber Power and America's National Security," U.S. Army War College, May 2012, <https://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-072.pdf>.
24. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," U.S. Department of Justice, May 19, 2014, <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>; "Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information," U.S. Department of Justice, December 20, 2018, <https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion>.
25. Miles Park, "Chinese, Iranian, and Russian Hackers Targeted Biden and Trump Campaigns, Google Says," *National Public Radio*, June 4, 2020, <https://www.npr.org/2020/06/04/869922456/chinese-iranian-hackers-targeted-biden-and-trump-campaigns-google-says>.
26. Sean Lyngaas, "Chinese Spies Hop from One Hacked Government Network to Another in Asia Pacific, Researchers Say," *CyberScoop*, May 7, 2020, <https://www.cyberscoop.com/naikon-china-hacking-check-point-australia-vietnam/>.
27. Justin Lynch, "China is Hacking the Same Countries It Trades With," *Fifth Domain*, August 17, 2018, <https://www.fifthdomain.com/international/2018/08/17/china-is-hacking-countries-is-trades-with/>.
28. Robert Rapier, "China Emits More Carbon Dioxide than the U.S. and EU Combined," *Forbes*, July 1, 2018, <https://www.forbes.com/sites/rpapier/2018/07/01/china-emits-more-carbon-dioxide-than-the-u-s-and-eu-combined/#5639df83628c>.
29. Mehari Taddele Maru, "Why Africa Loves China," *Al Jazeera*, January 6, 2019, <https://www.aljazeera.com/indepth/opinion/africa-loves-china-190103121552367.html>.
30. "Cyber Threats to Nordic Region," *FireEye*, May 2015, <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-nordic-threat-landscape.pdf>.
31. "China Says It's Not a Threat to Norway; Denies Cyber Espionage," *Reuters*, February 4, 2019, <https://www.reuters.com/article/us-huawei-tech-norway/china-says-it-is-not-a-threat-to-norway-denies-cyber-espionage-idUSKCN1PT23M>.
32. Vytautas Budzinauskas, "Nordic and Baltic countries face similar threats from Russia and China – interview," *LRT English*, November 4, 2019, <https://www.lrt.lt/en/news-in-english/19/1112835/nordic-and-baltic-countries-face-similar-threats-from-russia-and-china-interview>.
33. Dimitri Trenin, "Russia and China in the Arctic: Cooperation, Competition, and Consequences," *Carnegie Moscow Center*, March 31, 2020, <https://carnegie.ru/commentary/81407>.
34. Sara Peters, "What does China-Russia No-Hack Pact Mean for the U.S.?" *Dark Reading*, May 11, 2015, <https://www.darkreading.com/vulnerabilities---threats/advanced-threats/what-does-china-russia-no-hack-pact-mean-for-us-/d/d-id/1320365>.
35. Catalin Cimpanu, "Report: Chinese Hacking Group APT 40 Hides Behind Network of Front Companies," *ZDNet*, January 13, 2020, <https://www.zdnet.com/article/report-chinese-hacking-group-apt40-hides-behind-network-of-front-companies/>.

Attack-Based Network Defense

Major William North

ABSTRACT

The Department of Defense Information Network-Army (DODIN-A) is one of the largest and most complex networks in the world, and commanders are struggling to determine the effectiveness of their defensive posture as threat actors constantly attack the unclassified and classified networks. To gain a shared understanding of threats across its Defensive Cyber Operations-Internal Defensive Measures (DCO-IDM) and the cybersecurity community, the Army must establish a catalog of known and unknown threat techniques. This catalog would provide a list of analyzed threat techniques and potential mitigation actions so that Army forces spend less time reacting to the results of exploitations and more time defeating malicious actors. The catalog would also provide the foundation to support persistent penetration testing to provide a mechanism to find overlooked weaknesses, and to train analysts with real-world vulnerabilities. With this methodology in place, an Attack-Based Defense would establish an objective and quantifiable way to assess the effectiveness of cyber forces, inform commanders on how to employ cyber forces, provide business metrics for where cyber forces can improve, and ensure a common incident response across the enterprise.

INTRODUCTION

Recently there have been several highly embarrassing and entirely preventable penetrations into the Department of Defense Information Network (DODIN) conducted by DoD personnel such as the Attack the Pentagon program and the Ms. PacMan 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.



MAJ William North has served in the U.S. Army as a network engineer for 14 years. His last assignment was serving as the Network Defense Chief for U.S. Army Cyber. Before that, he served as a network engineer for the 335th Signal Command (Theater) (Provisional). He was honored with Meritorious Service Medals for his contributions to cyber and network operations. He is a distinguished graduate of the Intermediate Learning Education course and is currently a Ph.D. student at the University of Illinois at Urbana-Champaign.

Even though the tests were aimed at sections of the DODIN that do not affect the Army, one inevitably deduces that the defense of the DODIN and, by extension, the DODIN-A have room for significant improvement. A nation-state actor takes fewer than twenty minutes on average to start moving laterally after an initial compromise^[1] and the time between vulnerability disclosure and weaponization is nine days on average,^[2] the Army must take steps to improve network defense strategy and operations.

Army Regulation 10-87 tasks US Army Cyber Command with providing cyber support to combatant commanders and serving as the Cyber Security Service Provider (CSSP) for the DODIN-A.^[3] The full spectrum of cyber operations includes cyber-attack, exploit, defense, and security. The CSSP requirements are to identify, protect, detect, respond, and recover. Of these mission sets, the cyber operations security and defense with the CSSP pillars provide the broad guidance for the Army to conduct defensive cyberspace operations.^[4] In the Army, the principal Defensive Cyberspace Operations-Internal Defensive Measures (DCO-IDM) lead is the Cyber Protection Brigade with its service-assigned teams, and the principal for DODIN operations is the Network Enterprise and Technology Command (NETCOM). As noted in draft Army Field Manual 3-12, “Cyberspace defense actions conducted during DCO-IDM overlap with cyberspace security actions performed during DODIN operations.”^[5] Therefore, effective defense of the DODIN-A requires a continuum of effort between these principal units.

Unfortunately, the Army does not have the organizational structure and collective processes to knit these separate units together. The defense community does not have a common communications platform and utilizes a vast array of toolsets that have led to drastically different tactics, techniques, and procedures in different units. This muddled and confusing strategy frustrates efforts to develop a focused community and

limits the ability of defensive forces to respond to threats in an accurate and timely manner. Therefore, the Army must adopt a coordinated methodology supported by objective measures of performance (MOP), supported by key performance parameters (KPP), which assures commanders that the DODIN-A is properly defended against adversary activity and provides commanders situational awareness to make timely and accurate decisions.

FOUNDATIONAL ASSUMPTIONS

Asset Management

One underlying requirement for the Attack-Based Defense to work is that defensive personnel must have an accurate picture of the network they are defending – in other words, the foundation is hardware and software asset management. This ensures network operators have access to authorized devices and software and can detect unauthorized and unmanaged devices and software. Without understanding what is and is not on the network, defensive forces spend more time trying to understand terrain than in mitigating incidents on the network. Furthermore, having a standard asset management solution provides a box around expected behavior which enables analysts to determine anomalous behavior more quickly.

Data Management Strategy

The other underlying requirement is that analysts must capture the appropriate logs from all relevant data sources. Provided a minimum-security baseline (described below), network operators have a guide as to which data points are important, for how long data need to be stored, and how quickly those data points need to be ingested. This drives a robust data management strategy that incorporates the way an analyst formats and culls data, the development of the data fabric to facilitate the transport of data, and backbone infrastructure to support this data flow. Without protected and complete logging records, defensive forces are blind to the details of an attack and follow-on actions taken by the adversary.

Threats

To develop an objective and quantifiable approach to defense, the Army must start with understanding known and unknown threat techniques. For example, when defending against known threat techniques, cyber defenders should be able to tell the commander: how a threat technique works, where the risks lie in defending against that technique, how best to increase the security posture in response to that technique, how the Army will defend against that technique, and the potential impact on mission execution. For unknown threat techniques, defenders should be able to provide to the commander: potential avenues of approach for that technique and recommendations on how to increase the DODIN-A's security posture against that technique. For known threat techniques and potential unknown threat techniques, defenders need to be able to evaluate their effectiveness to monitor, detect, and respond to these threat techniques.

In defending the network, one cannot assume that 95 percent patching is good enough as a cyber adversary needs only to find one weak link to bypass the cybersecurity wall, take advantage of unmitigated vulnerabilities, and easily pivot from the initial entry point into the heart of the network. Therefore, a threat to any portion of the network is a threat to any other part of the network. We must analyze every threat technique from x_1 to x_n .

To understand the x_1 known threat technique (in the Attack-Based Defense Model, this is the base phase), an analyst must answer the following questions:

- ◆ Of what vulnerability is the x_1 threat technique taking advantage?
- ◆ What characteristics and attributes identify x_1 ?
- ◆ What is the behavior of x_1 ?
- ◆ What data can an analyst collect to detect the indicators and behavior of x_1 ?
- ◆ What does an analyst do when presented with a correlated event indicating a compromise?
- ◆ What is the triage priority of this event?
- ◆ Who else needs to know this information?

Further, an analyst must also consider all other known threat techniques and consider if there is overlap with x_1 . For example, consider x_2 known threat technique:

- ◆ Is it possible that the vulnerability, indicators, and/or behavior overlap with x_1 ?
- ◆ If so, does an analyst need to collect the data once or twice?
- ◆ Is there correlating information between x_1 and x_2 ?

The answers to these questions inform defensive forces how to detect, understand, and monitor threat techniques. An analyst will consolidate this threat technique dictionary into a single document to which all defensive forces have access for shared understanding. This document, known as the Minimum-Security Baseline (MSB), provides a catalog from which threat techniques are monitored, analyzed, and mitigated.

However, having an MSB does not guarantee that analysts will respond correctly once an analyst detects a threat technique. Persistent penetration testing (PPT) provides a way to regularly assess the completeness of the MSB and the ability of defensive forces to respond in an accurate and timely fashion to known and unknown threat techniques. PPT enables a continuous feedback loop in which red teams assess defensive forces against the MSB and identify areas for improvement, providing a mechanism to fold those recommendations back into the MSB that red teams validate in another assessment. This methodology supports a running estimate of known threat techniques against which defensive forces can and cannot defend;

indicates where to reinforce the network's defensive posture; allows red teams to test response time and actions of analysts; provides validated analytics, questions, rules, and signatures for detection; provides a playbook for response actions; and offers a continuous feedback loop that fuses DODIN operations, DCO-IDM, and threat intelligence.

When considering y_n unknown threat techniques, DCO-IDM forces are at a significant disadvantage. These types of threats include insider threat events, social engineering, and zero-day threats derived from intelligence sources. Although they are initially at a disadvantage, this method creates the ability to quickly push a y_n threat technique from being unknown into an x_n known threat technique through a deliberate and sustainable process. Additionally, it outlines a framework that enables DCO-IDM forces to hunt for adversaries on the network while providing a mechanism to ensure an analyst incorporates the selectors into the MSB.

ATTACK-BASED DEFENSE

This approach to threat techniques provides the structural foundation of the Attack-Based Defense method. It contrasts with the current way the Army approaches cyber defense, which is more akin to bumping into things to determine that something is amiss. To implement this Attack-Based Defense method, the Army should utilize the following three-tiered process:

Base Tier

The base tier is the threat assessment phase, and the main objective of this phase is to identify and characterize threats and package this information into the MSB. This phase underpins the Attack-Based Defense and requires technically and tactically sound analysts grouped into a DevOps Support Cell (DSC). The DSC's job is to translate the offensive cyber mindset to the Army's defensive posture. DSC analysts must possess skills that include scripting, security information and event management systems, offensive cyber operations, endpoint detection and response, and operating system logging. Due to the challenging variety of skill sets required, the cost to employ these individuals, and the need to develop an enterprise MSB, the DSC should reside at the highest organizational level possible. Additionally, leadership should insulate the DSC from day-to-day operations to ensure the team develops and disseminates high-quality content to DCO-IDM forces.

A key tool in the base phase is a testing environment. To create an MSB efficiently and effectively, the DSC will need to analyze threat techniques and run malicious code against an emulated Army network. The lab will provide analysts an environment that will not break the production environment and a sandboxed location in which to train against known threat techniques. Beyond traditional defensive operations, this lab will also provide numerous advantages to the Army, such as a collaborative environment that fosters progress and innovation of TTPs through research and development, a shared environment for new applications testing and evaluating new Commercial Off the Shelf (COTS) software on an open network that does not associate the process with the Army for operational security, an environment

that simulates actual base or enclave-level architecture unconstrained by DODIN-A security policy, and an avenue for Cooperative Research and Development Agreements (CRADA) which will improve ties with vendors for newest versions of software and faster technical support. In general, leadership should consider the lab as an internal resource in which all interested users can come to test new content, whether hardware or software, before recommending its installation or purchase.

The output of the base phase is an MSB that includes a catalog outlining what a threat technique does, the indicators and behaviors associated with that threat technique, a triage priority assignment, and the defensive techniques that should be employed against that technique. The MSB is tool and network agnostic so that an analyst can apply it to any network and provides the foundation for the Attack-Based Defense.

2nd Tier

The second tier applies the MSB to the tools used by defense analysts. This requires a dedicated red team and a defense analyst cell to deploy real-world threat techniques and to determine the effectiveness of the response with the tools available. During this phase, the MSB integration team develops the KPPs and MOPs that drive the defense response against a known threat technique. Sample KPPs are the time to detection, time to response, and the ability to assess x_n threat technique as x_n correctly. During the creation of the KPPs and MOPs, analysts should attempt multiple threat techniques simultaneously so that the aggregate DCO-IDM responses are in line with the individual KPPs and MOPs. If the response is sufficient, an analyst will pass that portion of the MSB, its tool-specific implementation, and the KPPs and MOPs to the third tier. If the response for x threat technique is insufficient, an analyst sends the threat technique response playbook back to the DSC for further analysis and refinement.

3rd Tier

The third tier takes the output of the second tier to create a shared understanding for the cyber defense community, enabling analysts to understand what an event means and how to respond by referencing the MSB. Essentially, this tier provides defensive forces a clear understanding of what the threat technique is and how to mitigate it (from the MSB), its expected response time (from the KPPs), and an objective way to measure performance. Further, it provides a foundation for red teams to conduct persistent penetration testing which easily and clearly provides the commander with a way to measure the effectiveness of his or her defensive forces and proactively find unknown threat techniques.

IMPROVING ON EFFECTIVENESS

Considering how well the defense community performs is difficult because there is not a standard set of tasks with adequate measures of effectiveness to conduct an assessment. Additionally, the defense community currently lacks a standard way to communicate about threat

technique response and how to convey to leadership the risk associated with an incident. Though there are several efforts throughout DoD to standardize policy and broad tasks,⁶¹ the Army has not adopted these efforts in a comprehensive strategy. Without such a framework, leaders cannot determine if the Army is effectively spending its limited resources for cyber defense.

Further, the lack of measures of effectiveness exacerbates the shortcomings of current effectiveness assessments, which amount to proving a negative. When the network is running without incident or, more likely, incidents are contained below the need for leadership involvement, leaders are easily lulled into complacency. However, when an incident does occur, leaders face a significant impact on operations during response actions. This whiplash between background noise and significant impact provides a false image of the work being accomplished behind the scenes. To overcome this, analysts need to show leadership dashboards with relevant and clear information that strikes a balance between hiding complexity and highlighting critical information that leads commanders to take both proactive and reactive actions.

Such dashboards are incredibly difficult to make without having clearly defined the tasks for cyber defense and a standard way of referring to threat techniques which I advocate through the MSB. Without it, the Army will continue to struggle to communicate effectiveness to leaders both proactively and reactively. Therefore, though the creation of the MSB requires significant investment and commitment, it is a necessary first step in unifying the community's efforts and being able to show concrete metrics that leaders use to understand how effective defensive forces are utilizing the holistic Attack-Based Defense approach.

OBJECTIVES OF AN ATTACK-BASED DEFENSE

The Attack-Based Defense provides a methodical approach to cyber defense. Without such an approach, the Army will continue to have an unorganized and haphazard approach to adversaries in the DODIN-A. The main objective of Attack-Based Defense is to provide a way to measure the effectiveness of defensive forces against known threat techniques through an MSB and a process to turn unknown threat techniques into known threat techniques quickly. The MSB provides the foundation for PPT, which emulates the threat technique and enables the feedback loop where unknown threat techniques turn into known techniques. Finally, an Attack-Based Defense provides an objective and quantifiable way to assess the effectiveness of defensive forces, inform commanders how to employ defensive forces, provide data on where the Army's defensive forces can improve their effectiveness, and ensure a common MSB across the enterprise.🛡️

DISCLAIMER

The views expressed in this work are those of the author 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. “First-Ever Adversary Ranking in 2019 Global Threat Report Highlights the Importance of Speed,” CrowdStrike, accessed April 16, 2020, <https://www.crowdstrike.com/blog/first-ever-adversary-ranking-in-2019-global-threat-report-highlights-the-importance-of-speed>.
2. “Think Fast: Time Between Disclosure, Patch Release and Vulnerability Exploitation — Intelligence for Vulnerability Management, Part Two,” FireEye, accessed April 16, 2020, <https://www.fireeye.com/blog/threat-research/2020/04/time-between-disclosure-patch-release-and-vulnerability-exploitation.html>.
3. U.S. Department of the Army, 2017, *Army Commands, Army Service Component Commands, and Direct Reporting Units: Army regulation 10-87*, paragraph 14-2.b.(2). “ARCYBER - Plans, executes, directs, and synchronizes assigned and authorized Joint and Service DODIN operations and defensive CO across the Army’s portions of the DODIN and, when directed, on other DODIN and non-DODIN networks;” paragraph 14-2.b.(8) “Serves as the Army’s principal Cybersecurity Service Provider (formerly Computer Network Defense-Service Provider).”
4. U.S. Department of the Army, 2020, draft, *Cyberspace Operations and Electronic Warfare: Field Manual 3-12*, paragraph 2-5. “Cyberspace actions used to defend blue cyberspace are actions employed through cybersecurity and defensive cyberspace operations-internal defensive measures (DCO-IDM).”
5. *Ibid.*, paragraphs 2-17.
6. Examples of methodologies are the Department of Defense Cybersecurity Services Evaluators Scoring Metric, and the United States Cyber Command Risk Assessment Methodology.

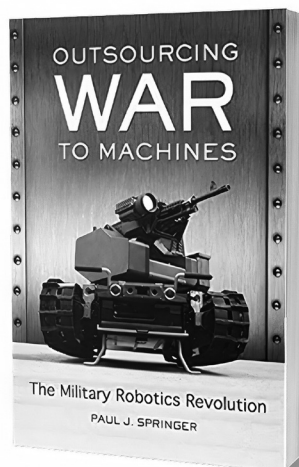
THE CYBER DEFENSE REVIEW

◆ BOOK REVIEW ◆

Outsourcing War to Machines: The Military Robotics Revolution

By Paul J. Springer

Reviewed by
Cadet Dylan Taylor
Major Mark Lesak



EXECUTIVE SUMMARY

Professor Paul J. Springer's book *Outsourcing War to Machines: The Military Robotics Revolution* "seeks to provide context to the rise and deployment of military robotics. It raises issues with the legality and morality of using these advanced systems and critiques the ways in which they have been used in recent conflicts" (3). This includes, but is not limited to: discussion regarding some of the very first machines deserving the title of "robot," case studies on robotic applications in the last few decades, speculation surrounding the role of military robotics in the future, and analysis of moral and ethical arguments concerning the use of lethal force by an autonomous system. In all, Springer leaves absolutely nothing out within these pages and provides an extremely thorough overview on the entire history of military robotics.

One minor issue with Springer's book, however, is that the details and information are a little overbearing at times. As a reader interested in the robotics, I do not need several pages dedicated to crossbows and gunpowder, for example. They certainly supported the argument at hand but mentions such as those could very easily be shortened without any loss of understanding. Regardless, Springer's superb historical insight provides an excellent foundation for higher-level discussion.

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



CDT Dylan Taylor is an Electrical Engineering major at the United States Military Academy. He graduated from Perkiomen Valley High School in 2018. CDT Taylor is a student member of the Institute of Electrical and Electronics Engineers (IEEE), vice president of West Point's Eta Kappa Nu Honors Society (HKN), and player on West Point's esports team. Upon graduation, CDT Taylor hopes to commission into the Army Cyber branch as an Electronic Warfare Officer. Before reporting to his first duty assignment, however, he would like to earn his MS degree in Electrical Engineering at MIT through either a Lincoln Labs or Draper Labs fellowship.

REVIEW

Springer begins his discussion by defining key terms such as “robot,” “drone,” “autonomy,” “artificial intelligence,” etc., to reduce the likelihood of misconceptions or misinterpretations which is very help helpful, especially for readers who may not be familiar with such terms. The remainder of the first chapter involves a concise background of the war on terror—by far the most relevant conflict to military robotics. In all, the introduction is set up very nicely and effectively prepares the reader for the rest of the book.

In the following chapter, Springer introduces the concept of revolutions in military affairs (RMAs) which refer to any “fundamental transformation in the means or methods of conducting warfare” (24). For example, innovations such as the phalanx, gunpowder, and the atomic bomb all completely changed the battlefield in their own respective eras. Springer then argues that robots are quickly becoming the next great RMA and that those who fail to embrace it will fall short of those that do, brilliantly citing several historical examples to support his argument.

This second chapter is a perfect example of Springer exercising his incredible wealth of knowledge, while losing focus on the application of military robotics: the chapter itself is very well written with copious amount of information, but spends a little too much time on examples that date back to ancient Greek warfare. While this approach may be interesting to some readers, it may be distracting to those who are solely interested in learning about modern robotics.



MAJ Mark Lesak is a Research Scientist for the Army Cyber Institute (ACI) at West Point. He is a 2009 graduate of the United States Military Academy where he majored in Mechanical Engineering and earned a MS degree from Colorado School of Mines in 2019 where he focused his research on robotics. Prior to conducting research as part of the Emerging Technologies team at ACI, he deployed to Iraq as the Fusion Intelligence OIC and later transferred to the Cyber branch where he led a Combat Support Team and took company command.

Structured in a very similar manner, Chapter Three provides an abundant amount of information dedicated to Ancient Egypt, Leonardo da Vinci, Nikola Tesla, and the Wright brothers. Albeit excellent historical summarization, the examples are once again a little excessive and not necessarily aligned with the purpose of the book as laid out in the introduction. The rest of the book, however, is very applicable to military robotics and covers topics ranging from morality and ethics to autonomous weapon systems employed today. Of particular note, Chapters Five and Seven discuss legal loopholes and malicious viruses, respectively, which were very informative and entertaining to read. Springer does warn that, as long as robotics are unregulated, certain individuals will hold an incredible amount of power. For example, the President of the United States can order the CIA to conduct drone strikes in the Middle East because the CIA is not bound by the Uniform Code of Military Justice nor do drones fall under the War Powers Resolution. In other words, technology appears to be advancing at a pace faster than the regulations surrounding it. This is just one of the many subtopics Springer covers in the book.

Stylistically, the author follows a very consistent organizational structure throughout *Outsourcing War to Machines*. This involves splitting chapters up into many subsections each with their own argument or topic sentence which he states directly. Then, the rest of each subsection contains a tremendous number of examples that ensures the reader understands the key point the author is claiming or the context of the situation. Finally, he restates the argument or topic sentence and moves on to the next subsection. At the end of each chapter, Springer ties everything back to the current state of military robotics. In all, the structure is very easy to follow and helps the reader digest the material.

CONCLUSION

Outsourcing War to Machines effectively summarizes the context and rise of military robotics all the way from ancient civilization to modern warfare. Even someone well-versed in this subject area can learn a lot from Springer's work. There is no doubt he conducted a lot of research to provide the most accurate information possible. The historical examples may be a redundant or excessive to some readers, but the book is very well organized and provides readers an excellent background to this latest revolution in military affairs. 🛡️

Title: ***Outsourcing War to Machines: The Military Robotics Revolution***

Publisher: Praeger Security International (2018)

Hardcover: 220 pages

Language: English

ISBN-13: 978-1-4408-3085-3

EISBN: 978-1-4408-3086-0

Price: \$63.00 (Hardcover)

\$59.85 Kindle Edition


THE CYBER DEFENSE REVIEW


CONTINUE THE CONVERSATION ONLINE

 CyberDefenseReview.Army.mil

AND THROUGH SOCIAL MEDIA

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

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

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



ARMY CYBER INSTITUTE ♦ WEST POINT



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