

# THE CYBER DEFENSE REVIEW

\*\*\*

Cyber Crime and Geostrategic Clash Over the Internet:  
Deputizing the Private Sector to Assist

*Admiral (Ret.) Dennis Blair  
Bud Roth*

Conceptualizing Cyberspace Security Diplomacy

*The Honorable Christopher Ford*



AI, Super Intelligence, and the Fear of Machines in Control

*Brian Mullins*

Information as Power: Evolving US Military Information Operations  
and Their Implications for Global Internet Governance

*Dr. Milton Mueller, Dr. Karl Grindal*

Timing Influence Efforts with Information Processing

*Dr. Joshua McCarty, Kaylee Laakso*

“Explicit” Bargains are Essential to Forming Desired Norms in Cyberspace

*Maj. Wonny Kim*

America’s Cyber Auxiliary: Building Capacity and Future Operators

*Lt. Col. (Ret.) Jeffrey Fair*

The Global Engagement’s Center’s Response to the Coronavirus Infodemic

*Maj. Neill Perry*

---

## INTRODUCTION

So...Anything Interesting Going On?

*Col. Jeffrey M. Erickson*

## BOOK REVIEW

*Bitskrieg: The New Challenge of Cyberwarfare*  
by John Arquilla

*Maj. Mathieu Couillard*



# THE CYBER DEFENSE REVIEW

◆ SPRING 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

### 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)

Dr. Michael Klipstein  
(Cyber Policy/Cyber Operations)

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. (P) 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  
University of Texas at Austin

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.

### PUBLIC AFFAIRS OFFICER

Maj. Joseph Littell

### KEY CONTRIBUTORS

Clare Blackmon  
Nataliya Brantly

Kate Brown  
Erik Dean

Debra Giannetto  
Carmen Gordon

Col. Michael Jackson  
Lance Latimer

Charles Leonard  
Alfred Pacenza

Diane Peluso  
Michelle Marie Wallace

### CONTACT

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

### SUBMISSIONS

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

### WEBSITE

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

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

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

This publication of the CDR was designed and produced by Gina Daschbach Marketing, LLC, under the management of FedWriters. The CDR is printed by McDonald & Eudy Printers, Inc. ∞ Printed on Acid Free paper.

## INTRODUCTION

**Col. Jeffrey M. Erickson**

9

So...Anything Interesting Going On?

---

## SENIOR LEADER PERSPECTIVE

**Admiral (Ret.) Dennis Blair  
Bud Roth**

15

Cyber Crime and Geostrategic Clash  
Over the Internet: Deputizing the Private  
Sector to Assist

**The Honorable Christopher Ford**

35

Conceptualizing Cyberspace Security  
Diplomacy

---

## PROFESSIONAL COMMENTARY

**Lt. Col. (Ret.) Jeffrey Fair**

57

America's Cyber Auxiliary: Building  
Capacity and Future Operators

**Brian Mullins**

67

AI, Super Intelligence, and the Fear of  
Machines in Control

---

## RESEARCH ARTICLES

**Dr. Milton Mueller  
Dr. Karl Grindal**

79

Information as Power: Evolving US  
Military Information Operations and  
Their Implications for Global Internet  
Governance

RESEARCH ARTICLES

<b>Maj. Wonny Kim</b>	99	“Explicit” Bargains are Essential to Forming Desired Norms in Cyberspace
<b>Dr. Joshua McCarty Kaylee Laakso</b>	115	Timing Influence Efforts with Information Processing
<b>Maj. Neill Perry</b>	131	The Global Engagement’s Center’s Response to the Coronavirus Infodemic

---

BOOK REVIEW

<b>Maj. Mathieu Couillard</b>	141	<i>Bitskrieg: The New Challenge of Cyberwarfare</i> By John Arquilla
-------------------------------	-----	---



# THE CYBER DEFENSE REVIEW

◆ INTRODUCTION ◆



## *The Cyber Defense Review:* So...Anything Interesting Going On?

Colonel Jeffrey M. Erickson



**A**s I read through the Spring CDR, I found that the war in Ukraine was on my mind and that I analyzed the articles through that lens. During my reading of each article, I kept asking myself the following:

- ♦ How does this relate to the current and evolving situation in Ukraine?
- ♦ Is Ukraine validating many of our assumptions of modern, multi-domain operations?
- ♦ Or is it a return to more traditional/conventional warfare?
- ♦ Finally, how are other adversaries, such as China, leveraging the situation to their own benefit?

While not written with Ukraine in mind, I think you'll find many relevant articles in this issue that highlight the need for continued thought leadership in cyberspace, which plays a crucial role in current and future competition and conflicts.

In our Leadership Perspective section, Admiral (Ret.) Dennis Blair (former U.S. Director of National Intelligence) and William "Bud" Roth, Esq. (781st Military Intelligence Battalion, U.S. Army) argue for the expansion of the role of the private sector in cybersecurity. They highlight historical examples where private companies have assisted with law enforcement activities and describe a three-tiered licensing system that would increase collaboration with the government and overall defensive capabilities. Additionally, the Honorable Christopher Ford (former U.S. Assistant Secretary of State for International

*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.

Security and Nonproliferation) in “Conceptualizing Cyberspace Security Diplomacy” provides a framework around the variables of information strength, partner trust, and operational consequence as a way to inform responses to threats. The graphical representation of his framework provides a visualization of potential outcomes.

We are excited to showcase two outstanding Professional Commentaries in the Spring CDR. In his article “America’s Cyber Auxiliary: Building Capacity and Future Operators,” Lieutenant Colonel (Retired) Jeff Fair (Vice President of Cybersecurity and Economic Development at the San Antonio Chamber of Commerce) argues for the creation of a cyber auxiliary corps like the Coast Guard Auxiliary Corps and the Civil Air Patrol. Both organizations were created during times of great change to create the necessary capacity to serve the nation while simultaneously inspiring new generations. Could we leverage a similar model for our current environment? While the article “AI, Super Intelligence, and the Myth of Control,” Brian Mullins (CEO, Mind Foundry) highlights the myths surrounding data, super intelligence, the role of humans in decision-making, and the barriers to achieving organizational intelligence.

Our Research Articles cover a variety of topics:

- ◆ In “Information as Power,” Dr. Milton Mueller (Georgia Institute of Technology’s School of Public Policy) and Dr. Karl Grindal (GIT’s School of Cybersecurity and Privacy) discuss the evolution of Information Operations within the US military, to include how it was implemented in the Cold War, Global War on Terror, and post-2016 election. They examine how the various services have approached information warfare and the possible friction points with the traditional US views on freedom of speech and the exchange of information.

- ◆ In “Explicit Bargains are Essential to Forming Desired Norms in Cyberspace,” Major Wonny Kim (Innovation and Information Operations Officer, 75<sup>th</sup> Innovation Command, U.S. Army) discusses the need for the US to better establish norms in cyberspace with respect to China through explicit policy, but also through actions. Failure to clearly define either could potentially lead to escalatory actions by both sides.
- ◆ In “Timing Influence Efforts with Information Processing,” Dr. Joshua McCarty (Purdue University Global) and Kaylee Laakso explain how information is sought and narratives are formed following crisis events. They present case studies that demonstrate the criticality of the first five days of information seeking and the eventual socialization of the information. By understanding the life-cycle of this process, it’s possible to leverage the window of opportunity to enable positive outcomes.
- ◆ Major Neill Perry (U.S. Air Force Reserves Intelligence Officer) discusses the US approach to disinformation in “The Global Engagement Center’s Response to the Coronavirus Infodemic.” He explores what worked and provides recommendations for the future.

Finally, Major Mathieu Couillard (Signals Officer, Canadian Armed Forces) provides an excellent review of John Arquilla’s *Bitskrieg: The New Challenge of Cyberwarfare*. Arquilla’s book seeks to define the complex current environment and provides some policy recommendations worth considering.

As Ukraine dominates the headlines, the ideas, concepts, and positions contained in this issue go beyond the current conflict to help our understanding of the enormous challenges and greater possibilities within cyberspace.♥



# THE CYBER DEFENSE REVIEW

◆ SENIOR LEADER PERSPECTIVE ◆



# Cyber Crime and Geostrategic Clash Over the Internet

*Deputizing  
the Private  
Sector to Assist*

---

Admiral (Ret.) Dennis C. Blair  
William “Bud” Roth

Over the past two decades, global society has shifted significant portions of its social and economic activities online. In the US alone, Internet Association experts estimate that Internet-based commerce accounted for about \$2.1 trillion, or 10% of GDP, in 2019. With this rise in economic and social activity, the world has witnessed a dramatic rise in cyber-attacks, mostly by criminal actors seeking to steal assets, defraud victims, and ransom decryption keys. One expert projects that by 2025, worldwide cyber-crime losses will reach a staggering \$10.5 trillion, making cyber-crime—were it a country—the world’s third largest economy.<sup>[1]</sup> For victims, the harm includes not only the cost of cleanup, but the loss of tangible assets such as stolen funds and fraudulent credit card charges, as well as harder-to-quantify figures for businesses that shut down operations or lose valuable intellectual property that finds its way into competitors’ hands.<sup>[2]</sup> Thus, the consequences for business owners and everyday citizens are severe. Yet progress in stemming the flow of cyber-attacks in the US seems stymied. The White House’s 30-nation meeting on ransomware in October 2021 was a promising initiative, but lacked any mention of private-sector active defense measures.<sup>[3]</sup> As noted in the 2016 “Into the Gray Zone” report co-authored by ADM Dennis Blair, one of this article’s authors, the US must take active steps not only to protect networks, but also to hunt down threat actors. Doing this at scale will require robust private sector participation. This article suggests one way to achieve this.

Currently, amid our inaction, private enterprise and government agency alike have suffered an unbroken string of malicious cyber intrusions that will continue unless we, as a nation, better galvanize and integrate the private sector into the nation’s defense. The theft

*Views and opinions herein are those of the authors.  
© 2022 Admiral (Ret.) Dennis Blair, William Roth.*



**Admiral (Ret.) Dennis Blair**, Knott Distinguished Visiting Professor of the Practice at the University of North Carolina at Chapel Hill, serves on the Energy Security Leadership Council and chairs the board of Security America's Future Energy. From 2014-18 Admiral Blair was the CEO and Chairman of the Board of the Sasakawa Peace Foundation USA. Previously, he served as Director of National Intelligence, President of the Institute for Defense Analyses, and Commander, U.S. Pacific Command. In addition, Admiral Blair served as Co-Chair for the GW Center for Cyber and Homeland Security 2016 report, "Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats." A graduate of the U.S. Naval Academy, Admiral Blair earned a master's degree in history and languages from Oxford University as a Rhodes scholar, and authored *Military Engagement: Influencing Armed Forces Worldwide to Support Democratic Transitions*.

of defense-related IP and national security secrets by government-sponsored hackers tangibly contributes to the geopolitical strategies and power of our adversaries. Military analysts point to China's leaps in military technology as, in great part, the result of China's rampant theft of US defense secrets and technology. The Pentagon's 2013 annual report to Congress noted that China uses stolen US defense technology to accelerate development of its weapons systems. A follow-up report leaked to the press identified the Aegis Ballistic Missile Defense System, F-35 Joint Strike Fighter, Littoral Combat Ship, and electromagnetic rail guns as systems whose plans were stolen by Chinese hackers.<sup>[4]</sup> This theft of defense technology is contributing to China's military confidence in pressuring the US and its allies across an array of tension points in Asia and elsewhere.<sup>[5]</sup> In short, nation-state hacking of US government (USG) and defense contractor networks has concrete and significant national security consequences.

As China and Russia recognize the strategic value of hacking our networks, they have mobilized hacker teams to identify networks with valuable US intellectual property or national security secrets, penetrate them, and steal the valuable IP or secrets.<sup>[6]</sup> Every year brings new examples of stolen US secrets, either from government agencies or companies. The OPM hack, Equinox breach, SolarWinds supply chain hack, and recent compromise of Microsoft Exchange systems are just a few major breaches that led to huge losses of national security and defense secrets.<sup>[7]</sup> Some of the compromised networks such as the Department of Homeland Security (DHS) and Department of Defense (DoD) networks, have implemented the strongest security protocols available, making the hackers' ability to operate undetected for months or even years all the more shocking.<sup>[8]</sup> Perhaps more disturbing, post-incident forensics confirm that US adversaries are still able to navigate networks freely and exfiltrate sensitive data, while avoiding detection.<sup>[9]</sup>



**William “Bud” Roth**, graduate of Dartmouth College, clerked at the Delaware Court of Chancery after law school and then began his federal career as an attorney with the Securities and Exchange Commission’s Office of Internet Enforcement. He served on the Department of Justice 9/11 Financial Crimes Task Force before leaving the SEC. Mr. Roth spent almost a decade with the Department of Defense supporting counter-terrorism operations, where he received a Defense of Freedom Medal and Meritorious Service Medal from the Department of the Army. Mr. Roth served as the Non-Resident Fellow for Cybersecurity at Sasakawa Peace Foundation before joining his current employer, the Army’s 781st MI Battalion. The authors previously coauthored, *A National Security Strategy for 5G (2020)* (presented at RSA 2020), and *WannaCry’s Lesson for the US-Japan Alliance*, *The Diplomat* (May 23, 2017).

As losses mount, the US has struggled to implement an effective deterrent policy.<sup>[10]</sup> Attempts to focus on protecting national security assets and critical infrastructure have failed, while leaving firms, agencies, and citizens who are not part of this subset of systems with little recourse to protect their networks.<sup>[11]</sup> While prioritizing critical infrastructure (and national security assets) is a logical next step in allocating limited resources, policymakers and security experts must be mindful that attacks on high-value targets are interwoven into a broader range of attacks supported at some level by adversaries seeking to disrupt the US economy or otherwise degrade public confidence in US and Western institutions. The onslaught of cyber-attacks our nation faces requires a more robust set of deployable defensive responses that effectively counter all attacks, whether state-sponsored or not, and for all networks, whether deemed critical infrastructure by the government or not. This requires more actors capable of responding. In short, increasing the number of assets available to defend against cyber-attacks is required to address the broader threat this nation faces. Activating private-sector defenders is the best way to do this.

This article takes the 2016 “Into the Gray Zone” report’s call for a larger private sector role a step further. We urge that private-sector capabilities be folded into a robust nationwide active defense of all US networks against any cyber-attack. This proposition is premised on the belief that criminal hacking is assisting our adversaries in three important ways:

- ◆ Providing noise that conceal sophisticated attacks by adversaries.
- ◆ Damaging Western assets and public confidence, consistent with our adversaries’ strategic goals.
- ◆ Exploiting sensitive networks targeted by adversaries and/or sharing the lead with state actors to exploit.

US adversaries are piggybacking on private sector criminals to compromise our networks and further their strategic goals, it only makes sense for the US to actively engage the private sector in countering these assaults on our nation. As a starting point, the next section examines in detail the ways our adversaries benefit from a criminal cyber threat.

### ***A. Noise that conceals sophisticated adversary attacks***

Cyber intrusions by Russian and Chinese military and intelligence sometimes track and other times differ from criminal behavior. For example, nation-state actors that steal national security secrets target federal agencies and government contractors or subcontractors because they hold secrets and defense-related intellectual property. Criminal actors seeking profit pursue a wider variety of targets, including hospitals and smaller firms unconnected to government. Yet, China's hacking blurs this distinction. For example, state-owned enterprises may direct government hackers to target IP and trade secrets of competitors in industries wholly unrelated to national defense.<sup>[12]</sup> Use of government resources for economic espionage is a longstanding sore point for the US, an issue President Obama stressed with President Xi during his 2015 visit.<sup>[13]</sup> But the problem does not stop there. Russia and China take it a step further by turning a blind eye to, and in many cases, hosting criminal hackers that target only western networks.<sup>[14]</sup> These adversaries deliberately provide safe havens and foster a cyber-crime ecosystem that targets US and Western networks. The sheer volume of such hacking attacks provides cover for our adversaries' cyber operations. Reacting to the widespread noise of criminal hackers consumes limited federal resources that could otherwise be available to counter the adversaries' best hackers, hackers who today may go undetected.

### ***B. Damaging Western Interests***

Russia and China are permitting—in some instances, encouraging—domestic hackers to attack Western targets.<sup>[15]</sup> Their permissive attitude may have originated from a belief that it was simply not worth the significant effort to stop criminal activity that only harmed Western economies and citizens.<sup>[16]</sup> For governments whose priority is domestic political stability and information control, curtailing criminals who target victims only in the West was logically a low priority.<sup>[17]</sup> Over time, perhaps because of complaints from the West, China and Russia became aware of the presence of these criminal hacker elements, and saw not a threat, but an opportunity.

Invented in the US as an open system outside government control, the Internet, from its beginning, has threatened authoritarian governments bent on strict controls over what the populace sees and thinks. Internet users around the world have always known that the Internet offers simple, hard-to-block ways for private citizens to sidestep censors and propagandists, and exchange news and ideas across borders.<sup>[18]</sup> Authoritarian governments have taken strong measures to control Internet usage: blocking seditious content, identifying disaffected citizens, and censoring content to favor official views and policies. Russia and China's rulers

see the Internet's explosive growth and free flow of information as not only a domestic threat to authoritarian control, but also as a core component of a Western-imposed, post-Cold War world order.<sup>[19]</sup> Their efforts to counter this Western threat go well beyond blocking portions of the Internet at the border; they include undermining the integrity of the Internet itself. Both countries leverage the open nature of the Internet to sow political discord and distrust in the West. One of their primary goals is to undermine Western confidence in the utility and safety of the Internet. Our adversaries see the Internet not only as a medium to subvert the West, but also as a symbol of the West that must itself be subverted.<sup>[20]</sup>

The tactical goal of subverting the Internet fits within our adversaries' overall strategic imperatives, and explains our adversaries' tolerance of criminal hacking activity against US and its allies. Criminal hacks such as the Colonial Pipeline hack or the Equifax credit report hack disrupt US society, create distrust of the Internet, and foster doubt about US abilities to defend American interests. This palpable impact has led adversaries to not just tolerate, but actively facilitate criminal hacking activity against US and Western interests.<sup>[21]</sup>

### *C. Acting as Hacker Proxies*

Analysis of serious hacks against US interests suggests that criminal hackers operating in China and Russia that target Western networks now receive various levels of state support, ranging from passive tolerance, to refusal to honor law enforcement requests for assistance, to active support and funding.<sup>[22]</sup> The sophisticated hacker group, Wicked Panda, began attracting US security firms' attention for their profitable targeting of gaming entities in 2013.<sup>[23]</sup> Beginning in 2015, Wicked Panda started targeting a broader array of industrial targets in the US, Japan, Germany and elsewhere, targeting that was more aligned with economic espionage goals of China's state-owned enterprises.<sup>[24]</sup> As the group's targets changed, they began using more sophisticated attacks. In 2016, analysts blamed Wicked Panda for a set of supply-chain attacks focused more on targets aligned with Chinese government strategic goals than on profits.<sup>[25]</sup> The Department of Justice (DOJ) unsealed indictments against five members of Wicked Panda in 2020, charging it with compromising networks of 100 firms, universities and agencies, stealing for profit, and illegally benefiting the Chinese government.<sup>[26]</sup> As then Deputy Attorney General Jeffrey A. Rosen put it, "The Chinese government has made a deliberate choice to allow its citizens to commit computer intrusions and attacks around the world because these actors will also help the P.R.C."<sup>[27]</sup>

Russia similarly has demonstrated tolerance of—if not collusion with—criminal hacking from its territories.<sup>[28]</sup> Indeed, the FBI seeks the arrests of Russia-based Maksim Yakubets and Igor Turashev for bank wire fraud and theft of over \$100 million from US banks and non-profits in 21 municipalities.<sup>[29]</sup> Russia persists in rebuffing arrest and extradition efforts.<sup>[30]</sup> Russian authorities know of, and authorities suspect at some level may be even complicit in, the criminal hacking activities of these two.<sup>[31]</sup> Not surprisingly, extradition is deemed highly unlikely as these criminal activities target US and Western countries only, and squarely advance Russia's

national security policy of weakening the US in response to perceived US interference with Russia's pursuit of its foreign-policy interests.<sup>[32]</sup> In fact, the Atlantic Council reports that Yakubets consults with Russia's Federal Security Service (FSB).<sup>[33]</sup> Here, the criminal Internet activity advances Russia's foreign-policy interest in weakening the US. It does this by degrading the public's trust in the Internet as a medium to transact business or conduct social activities, as well as degrading confidence in the ability of the US and Western governments to effectively defend their networks.

## **AN EFFECTIVE US RESPONSE**

Chinese hackers ignored President Xi's 2015 promise to President Obama to refrain from cyber-based economic espionage. The lack of follow-through exemplifies our challenge in compelling adversaries to curb criminal hacking against US targets. Policymakers have invoked several measures to dissuade adversaries from attacking US and Western networks. In addition to the Obama-Xi commitment, the US has rolled out the DoD "Defend Forward" strategy, DOJ "name-and-shame" indictments of overseas hackers, and trade sanctions.<sup>[34]</sup> Yet, cyber-attacks continue, undeterred, if not even greater than before.<sup>[35]</sup> The next section examines this threat with our view that even a whole-of-government response is not big enough to make a difference, and why we believe the private sector must be engaged in this effort.

### ***A. Historical Precedent For Private Sector Engagement in Enforcement***

Even when working collaboratively, the USG collectively lack the manpower to sift through the millions of cyber-attacks on US networks each month, much less flag and focus on the significant ones.<sup>[36]</sup> Indeed, the federal government is only able to identify and respond to a small handful of cyber incidents at any given moment, and local governments are even less effective. Large cities have recently begun working on a much-needed first-responder capability for cyber-attacks, but this effort focuses primarily on threat intelligence and incident response.<sup>[37]</sup> State and local law enforcement capabilities are quite limited, especially their Internet investigative capabilities, and their ability to pursue overseas hackers is almost non-existent. In short, the USG responses amount to no more than a drop in the bucket given the magnitude of this growing threat. This explains why US actions to date have come up short in meaningfully impacting the cost/benefit analysis of adversary governments and the criminals they host.

We believe it highly unlikely that the USG can ever develop a cyber investigative and retaliatory mechanism that effectively deters the myriad threat actors operating from *de facto* safe havens in Russia, China, and elsewhere. To build a defense and deterrence mechanism on a scale adequate to the challenge, the USG must leverage the private sector. We propose doing that by deputizing cyber security firms to hunt down the cyber attackers hitting US networks. There is a rich array of historical precedents for doing this.

### ***1. Bounty Hunters***

The War of Spanish Succession from 1702-13 and civil unrest in the Bahamas led to flourishing piracy in Caribbean waters.<sup>[39]</sup> England's King George I responded with naval force and promises of clemency that had the unintended effect of pushing the pirates to new waters off the coast of the Carolinas.<sup>[40]</sup> British colonial forces lacked the funding and personnel to counter this growing threat, which in the mid-1700's led colonial authorities in Charleston and elsewhere to offer bounties.<sup>[41]</sup> The idea was to entice commercial ship owners with sufficient weaponry and skilled sailors to hunt down and capture pirates marauding off colonial America's shores. These so-called bounty hunters became a critical part of the English response to piracy in the colonies and the Caribbean. Bounty hunters were responsible for capturing or killing "The Gentleman Pirate," Stede Bonnet, Blackbeard, Calico Jack, and John Roberts.<sup>[42]</sup> Rewarding private citizens for taking out pirates with a share of the pirates' stolen loot was controversial, but this practice allowed outgunned colonies to quickly build up a maritime force to the scale needed to counter the piracy threat, and provided a critical and timely solution to a crisis.

The effective role of privateers in fighting piracy as well as acting as naval mercenaries in time of war was in the minds of America's revolutionaries when they drafted the US Constitution.<sup>[43]</sup> Specifically, they added in Article I, Section 8, authority for Congress to "grant Letters of Marque and Reprisal," a clause commonly understood to permit the USG by act of Congress to hire privateers to interdict vessels of a warring state as well as pirates.<sup>[44]</sup> This authority can be extended to activities in international or foreign seas as well as US waters, leading some to suggest that cybersecurity firms be issued Letters of Marque to pursue criminal hackers,<sup>[45]</sup> although this suggestion has met much skepticism from legal and foreign policy experts.<sup>[46]</sup> We do not agree with the critics who fear cybersecurity firms will run amok in overseas networks, taking systems down in ways that the USG would never do and with diplomatic consequences that outweigh the deterrent impact of their actions,<sup>[47]</sup> and believe that the risks of this approach can be effectively mitigated. Indeed, as the next example demonstrates, private-sector actors can be deputized in ways that preserve judicial oversight and compliance with legal processes designed to protect legal and constitutional rights.

### ***2. Pinkerton Detectives***

Railroads in the western territories of the US faced growing lawlessness around the time of the Civil War. Living on the edge, some settlers turned to crime to survive.<sup>[48]</sup> Train robbery was lucrative, and at one point, a train robbery occurred once every four days.<sup>[49]</sup> Frontier towns appointed sheriffs to keep the peace, but they had little time or incentive to investigate train robberies taking place far from the outskirts of town, leaving railroads to fend for themselves.<sup>[50]</sup> In the 1850s, Illinois Central Railroad hired Allen Pinkerton to guard its railways and depots,<sup>[51]</sup> and fortuitously, hired a young attorney, Abraham Lincoln, to help

manage Pinkerton's efforts. Although on the railroad's payroll, Pinkerton detectives became *de facto* railway police. Unlike state and territorial authorities, they rode the train across borders and arrested bandits wherever caught.<sup>[52]</sup> In their heyday, Pinkerton detectives were the bane of railway bandits, infiltrating and bringing the Reno gang to justice as well as forcing Butch Cassidy and the Sundance Kid to flee to Argentina.<sup>[53]</sup> The Pinkerton detectives successfully employed what we now consider to be the inherently governmental authority of police arrest as well as undercover investigations to put in place a law enforcement capability to protect the railroads that the territories could not provide. Without this, the railroads could not adequately protect passengers and freight, or avoid serious operational disruptions.

It is worth noting that President Lincoln later used Pinkerton as his personal security and as an intelligence asset in the Civil War, helping cement Pinkerton's role as a trusted agent for the government and establishing precedent for entrusting private sector firms with highly sensitive government operations.<sup>[54]</sup> Unfortunately, Pinkerton detectives were later used to spy on and break up unions,<sup>[55]</sup> a low point in Pinkerton's history,<sup>[56]</sup> which should serve as a reminder that private firms charged with carrying out inherently government activities must be subject to the same rigorous oversight and judicial processes we require for government authorities.

Ultimately, use of private sector railway police made its way into the nation's national railway charter. Congress authorized Amtrak, a federally created corporation, to hire and deploy its own railway police.<sup>[57]</sup> Amtrak police officers attend training at the Federal Law Enforcement Training Centers or an equivalent state school. Amtrak police exercise arrest authority<sup>[58]</sup> and must afford citizens the same constitutional protections that govern normal police officers (Miranda warnings, Fourth Amendment rights, etc.).<sup>[59]</sup> We believe that private cybersecurity firms can be similarly engaged in the fight against cyber-attacks, armed with those authorities needed to pursue cyber intruders, and legally bound to honor the protections accorded to individuals suspected of hacking or of owning infrastructure wittingly or unwittingly exploited by criminals.

### ***B. Employing Private Security Firms to Hunt Down Hackers***

The US cybersecurity industry (with revenue estimated at \$54 billion in 2021)<sup>[60]</sup> is far larger than the USG's cybersecurity detection and incident response assets will ever be. It also possesses network defense talent and skills at a scale that the USG never could achieve. So, while these firms are already operating within private networks to protect them and to conduct forensic investigations into intrusions, they are prohibited from the more proactive elements of active defense. Private sector firms that pursue intruders beyond the client's network enter a murky legal realm. They risk violating Internet Service Provider's terms of service, state, and federal law, as well as the law of foreign states whose networks they traverse.<sup>[61]</sup> Yet active pursuit is where the government's capability gap hurts the US the most. To correct this, as with Pinkerton and the bounty hunters, the US cybersecurity industry should be authorized and incentivized to actively engage in hunting down malicious cyber

actors. Ability to chase down hackers in real time and identify their operational platforms, infrastructure and identity would be dramatically improved if private-sector hunters have US broader authorities. Private sector real-time tracking capability will greatly enhance the ability of the US to defend networks and deter attacks. As used here, real-time tracking is analogous to police crossing state lines chasing a suspect. This sort of hot pursuit authority would allow private sector defenders can cross borders and penetrate suspects' systems<sup>[62]</sup> is the USG's best way to build a rapid response mechanism scaled to the magnitude of the threat and with the means to hunt down, thwart, and otherwise deter the many bad actors that threaten the US now.

## PRIVATE SECTOR DETECTIVES AND PRIVATEERS

The Internet, fundamentally a creation of the West, promotes the free flow of information and low-cost commercial transactions at a scale never before possible.<sup>[63]</sup> It is integral to today's world order and acts as a medium for global communications and trade.<sup>[64]</sup> Protecting it aligns not only the USG's priorities, but also with the priorities and interests of the US private sector. Responsibly incorporating the private sector more actively into the cyber fray will require effective governance to avoid certain dangers. First and foremost is the profit motive, the concern that private firms might abuse their governmental authorities to pursue profits.<sup>[65]</sup> Secondly, there is the risk that activities legal here in the US would violate the laws of other countries, thereby exposing US firms to overseas law enforcement or civil actions.<sup>[66]</sup> Third, there is the possibility that a deputized private sector entity could unwittingly cause serious harm to a third-party or third-party network mistakenly suspected of being the criminal. Fourth, there is the need to avoid chaos by deconflicting the sorts of operations proposed here with overlapping actions by government agencies and other licensed private actors<sup>[67]</sup> Finally, there is the danger inherent in pursuing a network intruder who is part of a state-sponsored group.<sup>[68]</sup>

### *A. Profit Motive*

Private firms can be aligned with the national interest in several ways. For example, licenses and contracts can be crafted to align profit with national interest. Licenses would delineate required personnel qualifications, authorized and unauthorized activities, activity reporting, and periodic requalification. The licensed private firm could then solicit business with private companies to protect their networks, offering enhanced services not previously possible without the license. The commercial value of providing customers the enhanced services should, in turn, attract more business for licensed cyber security firms and, as with the railways and Pinkerton detectives, drive deployment of a much larger cadre of threat hunters to protect private sector assets. In the aggregate, this would achieve the national goal of protecting US networks. An important component of such a scheme would be the active, ongoing oversight of licensed firms, to ensure effective accountability. Private firms

would be required to obtain, either directly or through a federal partner, judicial and/or executive approvals necessary to fully protect the rights of US citizens and minimize impacts on third parties.<sup>[69]</sup>

### ***B. Overseas Investigations***

Actions by licensed private cyber defenders beyond US borders invariably will implicate other nations' laws. Tracking a hacker across multiple hops often requires logging onto machines in multiple jurisdictions. Understanding, much less abiding by each country's laws, poses a real challenge, and violations raise the specter of civil liability or criminal prosecution.<sup>[70]</sup> While this risk is real, it can be mitigated by allowing firms to operate under the same authorities that allow the government to do this. It can also be reduced by working with friendly nations to create common rules of the road for active defense by private companies, particularly when defenders are in hot pursuit of a hacker.<sup>[71]</sup> Legislation that protects defenders in hot pursuit from prosecution overseas may also be desirable. Finally, firms and their employees, like government employees, must accept some risk that their activities may make them targets of overseas investigations and impact their ability to travel freely.<sup>[72]</sup>

### ***C. Deconfliction and Government Oversight***

Private sector firms must not have free rein to hack into any machine suspected of housing a malicious hacker's activities. In the case of active, ongoing intrusions, an immediate hot pursuit authority is much needed, but must be granted with strict limits on authorized behavior and with immediate or almost-immediate reporting requirements to the proper deconfliction authority. In some instances, a private firm's use of a particular law enforcement tool, such as surreptitious entry, would require executive branch or judicial approval. In other words, as with Amtrak police, a private firm invoking special powers would be subject to the same legal restraints that govern federal agents. These controls and the preparation required to obtain judicial or executive branch approvals would reduce the risk of harm to innocent parties by forcing firms to explain themselves to a third party before acting. If the judge or oversight body agrees the proposed activities are justified then, and only then, would they coordinate and deconflict with ongoing operations by other private firms and federal agencies.<sup>[73]</sup>

### ***D. Active Federal Management***

As noted before, there are situations where network intruders breaking into private US networks are state actors.<sup>[74]</sup> Although in one reported instance, an individual took down North Korea's entire Internet in retaliation for being hacked by North Korean spies, we recognize that most firms lack the resources and risk tolerance to take on a hostile government.<sup>[75]</sup> Yet, if we deputize private sector firms to pursue threat actors, some of them will inevitably end up chasing state-sponsored actors. When this happens, it is crucial that the government

and licensed private firms be in communication, so that the government can step in and take over pursuit as warranted. The final section of this article proposes a task force designed to do exactly that.

## CYBER ACTIVE DEFENSE TASK FORCE

The federal government should create and empower a private-sector cadre with the proper authorities and the proper oversight to conduct active defense of US networks. This Cyber Active Defense Task Force or CADTF should be overseen by the Office of the Director of National Intelligence with representatives from NSA, CISA, DoD and FBI. They would license and oversee private firms authorized to use active defense tools normally reserved to the government. We use the term “license,” but the government-private sector relationship can be contractual, with each firm meeting stringent qualifications to be awarded a contract.<sup>[76]</sup> The end result of using contracts is similar to licensing, but might obviate a need for legislation.

This CADTF, operating from regional offices, would issue licenses (i.e., contracts) to qualified private sector parties authorizing specific permissive active defense measures.<sup>[77]</sup> To facilitate licensee governance, we envision the CADTF would issue three tiers of licenses:

- ◆ **Hot pursuit team:** These licensees would work for commercial (or government clients), protecting their networks as private cybersecurity firms already do, and further authorize pursuit of network attackers into a client’s network.
- ◆ **Cyber detectives:** These licensees would investigate threat actors, using special tools such as undercover operations and surreptitious entry (with proper executive or judicial approvals, as required).
- ◆ **Network operators:** These licensees would assist regional CADTF officers in managing local hot pursuit teams and cyber detectives, sharing intelligence with various private and public sector counterparts, and setting up infrastructure for regional hot pursuit teams and cyber detectives to use.

A core responsibility of CADTF personnel in each region would be to define required skills and capabilities for each tier of licensees, and to assess on a recurring basis whether licensees were maintaining those skills and qualifications.

### *A. Hot Pursuit Teams*

As with the Pinkerton detectives, hot pursuit teams would work for private sector clients, protecting their networks, but would possess the legal authority to pursue cyber-attackers. Hackers currently can break into networks, then flee across a border or into a third-party network, compelling victim companies and even state authorities to cease pursuit.<sup>[78]</sup> A hot pursuit license would give the private-sector cyber defender an authority analogous to a police chase. When a state trooper chases a suspect across state lines or into a house, the

trooper does not need to give up the chase but may continue, depending on the nature of the suspected crime and other factors so long as a hot pursuit continues. Network defenders must similarly be empowered to traverse networks across the US and the globe to collect evidence while responding to an ongoing intrusion. A hot pursuit team could follow an intruder across the Internet wherever the intruder goes, collecting evidence on the hacker, its machines, tools, and infrastructure. Eventually, the intruder will disappear behind a firewall or secure host for which there is no obvious access, and the chase must stop. In most cases, this is where hot pursuit would end. While some might argue that such a chase is already legal and already undertaken by private firms tracking stolen data, there is some ambiguity in the law when it comes to scanning hosts and looking for vulnerabilities or other unauthorized means of entering a network or logging onto a host. Also unclear is the consequences of violating Internet Service Providers' terms of service, and the laws of any particular nation implicated. Within clearly defined limits, the USG would authorize hot pursuit teams to pursue intruders across third-party networks.

In the rare situations where the hot pursuit team identifies a vulnerability by which to gain access to the intruder's host or secure network,<sup>[79]</sup> the CADTF would provide rapid consideration of a request by the team to grant immediate access to the intruder's machine and collect useful information. It would be incumbent, however, on the hot pursuit team to communicate with its CADTF point of contact at the outset of the hot pursuit, reporting their progress and seeking guidance on next steps. A CADTF official could then seek judicial or other required approvals needed before the hot pursuit team would be authorized to access to the intruder's machine. Alternatively, the CADTF official could, upon obtaining required approvals, bring in a government team or a cyber detective team (see below) to take operational control. Either way, the goal would be to immediately enter the intruder's machine or network and harvest evidence about keyboard operators, hacker tools, stolen data, and other evidence of wrongdoing. While taking retaliatory action would generally be barred, a hot pursuit team might request approval to delete copies of customer data if the data clearly confirmed theft from a client.

### ***B. Cyber Detectives***

As critical as hot pursuit authorities are, intruders rarely can be traced in real time beyond the first secure device.<sup>[80]</sup> Getting past the intermediate cut outs that hackers use to obfuscate their true origins requires significant fact gathering, analysis, and operational planning. By the time that process concludes, hot pursuit is long past, which gives rise to the need for the private sector to play a detective-like role. Like the Pinkerton detectives, cyber detective licensees would be empowered to use law enforcement authorities in their investigation of suspected criminal hacker groups. These would include undercover operations, running informants, reconnaissance, and surreptitious entry. Cyber detectives would work with various CADTF counterparts to develop or even execute a scheme of maneuver and must be

prepared to follow up on actionable leads generated by hot pursuit teams. Cyber detectives' activities would be subject to the same judicial and executive branch oversight applicable to a federal agent conducting the same activity. For example, with advance authorization, the cyber detective could use hacking tools to penetrate suspects' machines and collect evidence, or undertake undercover sting operations.

These cyber detectives would honor the same legal restrictions and judicial reviews governing government personnel and answer to the CADTF's deconfliction mechanisms. While risk is never totally eliminated, a cyber detective risk exposure should not exceed that of a federal agent doing the same task. Authorizing the private sector via cyber detective licenses to fulfill this role, however, acts as a force multiplier, greatly increasing the US' ability to pursue intruders, collect evidence of crime, and deter future attacks.

### *C. Network Operators*

Finally, we propose a third tier of licensee, the network operator, who would perform an infrastructure and management role. The need to build out a nationwide response would soon out-scale the USG's ability to manage licensees. CADTF should have regional offices that employ network operators to help manage their operational activities. In each region, CADTF government personnel, working in tandem with network operators, would perform the following functions:

- ◆ Build an infrastructure from which cyber detectives and, to some extent, hot pursuit teams, would operate.
- ◆ Provide a platform by which local licensees could communicate with the CADTF and other licensees.
- ◆ Act as a local or specialized analytical hub focusing on specific needs like local infrastructure protection and the regional threat landscape.
- ◆ Interact with CADTF teams nationwide, sharing information and operational plans.
- ◆ Manage sensitive taskings entrusted to the region's private sector licensees.

To perform these roles, the network operator licensee must be fully cleared and possess the sophistication and professionalism to act impartially towards other licensees and interact with the CADTF at the highest and most sensitive levels. Because network operators would play a regional role, and not only private firms, but state or local law enforcement can also play this role, thereby allowing for a more effective state and local first responder response to cyber-crime. One variation on this would involve National Guard units that, acting on behalf of the unit's home state, use either its inherent federal authorities or a CADTF detailee role, to spearhead local efforts to defend local networks and investigate intruders. Ultimately, such network operators, supporting a regional CADTF presence would permit a more dispersed and robust defensive ecosystem than we have now with only federal resources.

#### *D. Cyber Active Defense Task Force Management*

To ensure that licensees maintain the required qualifications and conduct themselves in accordance with the law, government personnel would always lead or oversee CADTF operations. It is essential the government officials perform these four roles:

- ◆ Adjudicate license applicant's qualifications and audit them periodically as licensees.
- ◆ Monitor licensees' activities to minimize counterintelligence and/or operational risk as well as compliance infractions.
- ◆ Share threat information in real time among CADTF agency members, licensees, and other partners to increase situational awareness and build actionable leads for all.
- ◆ Deconflict CADTF activities with other government activities.<sup>[81]</sup>

Under this management scheme, private sector licensees would be subject to proper oversight and could greatly expand our ability to counter the crippling number, size, and sophistication of cyber-attacks faced by the US.

### **CONCLUDING THOUGHTS**

There is strong, bipartisan resolve to thwart our adversaries ever evident ability to intrude upon US networks and steal or destroy our digital assets. This article proposes a way to counter this trend, but its implementation might, for some parts, will require legislation. To remain effective for the long term, such legislation should refrain from rigidly defining either the threat or the solution. Technology evolves at warp speed and many technical, legal, and practical lessons will be learned as private-sector cyber defenders enter the fray. Effective legislation should articulate precise authorities and limits, but leave executive branch personnel with flexibility in managing the public-private active defense partnership proposed here.

Our proposal would dramatically increase the number of active defenders available to fend off cyber-attacks. Across the nation, hot pursuit teams would operate inside client networks, guarding against intrusions, but would be empowered to move outside their defended networks, when attacked, to track intruders as far back as possible. Cyber detectives would engage in the long-term effort to identify and hunt down malicious actors, using law enforcement tools such as undercover operations and surreptitious entry when necessary. Finally, network operators would maintain the regional infrastructure required to house this public private partnership of active cyber defenders across the US. These three tiers of federal licensees would act as a force multiplier, bringing in a larger number of active network defenders than the government could ever provide.

The overriding goal of this article is to advance the operational need for and strategic value of bringing the private sector into a deeper and wider partnership with the government in defending our nation's increasingly imperiled networks. Without robust private sector augmentation, federal resources are simply inadequate to respond effectively and counter the millions of cyber-attacks that take place every month. US networks lie heavily in the private sector. To get this job done right, the private sector must shoulder a greater share of the burden of actively defending these networks. Our adversaries are fully engaged with criminal private sector elements whose activities undermine our citizens' ability to enjoy and rely on the Internet. We must find ways to deputize and otherwise entrust our enormously talented private sector to counter them. The USG needs the private sector as a full partner in hunting down malicious actors and taking them offline.🛡️

## NOTES

1. Steve Morgan, Editor-in-Chief, Special Report: Cyberwarfare in the C-Suite, Cybersecurity Ventures (Sausalito, CA, November 13, 2020), <https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/>.
2. See, for example, IBM Security, “Cost of a Data Breach Report 2021” (July 2021), Ponemon Institute, November 12, 2021, [https://www.ibm.com/security/data-breach?mhsrc=ibmsearch\\_a&mhq=data%20breach](https://www.ibm.com/security/data-breach?mhsrc=ibmsearch_a&mhq=data%20breach).
3. Briefing Room, White House, “FACT SHEET: Ongoing Public U.S. Efforts to Counter Ransomware,” October 13, 2021, <https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/>.
4. Sam LaGrone, “Report: China Hacked Two Dozen U.S. Weapon Designs,” *USNI News* (May 28, 2013), <https://news.usni.org/2013/05/28/report-china-hacked-two-dozen-u-s-weapon-designs>.
5. Ibid.
6. See Staff, “Significant Cyber Incidents,” Center for Strategic & International Studies, November 13, 2021, <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>.
7. Josh Fruhlinger, “The OPM hack explained: Bad security practices meet China’s Captain America,” CSO Online (February 12, 2020); Josh Fruhlinger, “Equifax data breach FAQ: What happened, who was affected, what was the impact?” CSO Online (February 12, 2020); Saheed Oladimeji & Sean Kerner, “SolarWinds hack explained: Everything you need to know,” TechTarget (June 16, 2021); and Kate Conger & Sheera Frenkel, “Thousands of Microsoft Customers May Have Been Victims of Hack Tied to China,” *The New York Times* (August 26, 2021), <https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html>, <https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html>, <https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know>, <https://www.nytimes.com/2021/03/06/technology/microsoft-hack-china.html>.
8. Staff, “The Biggest Hacks of 2021 (So Far),” *Gizmodo*, November 13, 2021, <https://gizmodo.com/the-biggest-hacks-of-2021-so-far-1847157024/slides/1>.
9. David Sanger, Nicole Perloth, and Eric Schmitt, “Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit,” *The New York Times* (December 14, 2020), <https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html>.
10. COL Timothy M. McKenzie, “Is Cyber Deterrence Possible?” Air Force Research Institute Papers (January 2017), [https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/0/0004\\_MCKENZIE\\_CYBER\\_DETERRENCE.PDF](https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/0/0004_MCKENZIE_CYBER_DETERRENCE.PDF).
11. Adm. Dennis C. Blair, Hon. Michael Chertoff, Frank J. Cilluffo, & Nuala O’Connor, “Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats,” 4, Center for Cyber & Homeland Security, George Washington University (October 2016), <https://wayback.archive-it.org/5184/20190103002934/https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf>.
12. Department of Justice, “U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage,” press release (May 19, 2014), <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>.
13. Scott W. Harold, “The U.S.-China Cyber Agreement: A Good First Step,” RAND blog (August 1, 2016), <https://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html>.
14. Tim Maurer, “Why the Russian Government Turns a Blind Eye to Cybercriminals,” Carnegie Endowment for International Peace (February 2, 2018), <https://carnegieendowment.org/2018/02/02/why-russian-government-turns-blind-eye-to-cybercriminals-pub-75499>.
15. See, for example, Katie Benner & Nicole Perloth, “China-backed Hackers Broke into 100 Firms and Agencies, U.S. Says,” *The New York Times* (September 16, 2020), <https://www.nytimes.com/2020/09/16/us/politics/china-hackers.html>; Bobby Allyn, “Russian Hacking Group Evil Corp. Charged by Federal Prosecutors in Alleged Bank Fraud,” *NPR* (December 5, 2019), <https://www.npr.org/2019/12/05/785034567/russian-hacking-group-evil-corp-charged-by-federal-prosecutors-in-alleged-bank-f>.
16. Tim Maurer, “Why the Russian Government Turns a Blind Eye to Cybercriminals,” Carnegie Endowment for International Peace (February 2, 2018), <https://carnegieendowment.org/2018/02/02/why-russian-government-turns-blind-eye-to-cybercriminals-pub-75499>.
17. Ibid.

## NOTES

18. See Shanthy Kalahil, “Internet Freedom: A Background Paper,” Aspen Institute (October 2010), [https://www.aspeninstitute.org/wp-content/uploads/files/content/images/Internet\\_Freedom\\_A\\_Background\\_Paper\\_0.pdf](https://www.aspeninstitute.org/wp-content/uploads/files/content/images/Internet_Freedom_A_Background_Paper_0.pdf).
19. Scott Jasper, “Assessing Russia’s role and responsibility in the Colonial Pipeline attack,” Atlantic Council (June 1, 2021), <https://www.atlanticcouncil.org/blogs/new-atlanticist/assessing-russias-role-and-responsibility-in-the-colonial-pipeline-attack/>.
20. Ibid.
21. Ibid.
22. Joseph Marks, “The Cybersecurity 202: The U.S. and allies are taking a stand against Chinese hacking. Here are three takeaways,” *The Washington Post* (July 19, 2021), <https://www.washingtonpost.com/politics/2021/07/19/cybersecurity-202-us-allies-are-taking-stand-against-chinese-hacking-here-are-three-takeaways/>.
23. Katie Benner and Nicole Periroth, “China-backed Hackers Broke Into 100 Firms and Agencies, U.S. Says,” *The New York Times* (September 16, 2020), <https://www.nytimes.com/2020/09/16/us/politics/china-hackers.html>.
24. Ibid.
25. Ibid.
26. Ibid.
27. Ibid.
28. Matt Burgess, “Leaked Ransomware Docs Show Conti Helping Putin From the Shadows,” *Wired* (March 18, 2022), <https://www.wired.com/story/conti-ransomware-russia/>.
29. Bobby Allyn, “Russian Hacking Group Evil Corp. Charged by Federal Prosecutors in Alleged Bank Fraud,” NPR (December 5, 2019), <https://www.npr.org/2019/12/05/785034567/russian-hacking-group-evil-corp-charged-by-federal-prosecutors-in-alleged-bank-f>.
30. Ibid.
31. Ibid.
32. Scott Jasper, “Assessing Russia’s role and responsibility in the Colonial Pipeline attack,” Atlantic Council (June 1, 2021), <https://www.atlanticcouncil.org/blogs/new-atlanticist/assessing-russias-role-and-responsibility-in-the-colonial-pipeline-attack/>.
33. Ibid.
34. Scott W. Harold, “The U.S.-China Cyber Agreement: A Good First Step,” RAND blog (August 1, 2016); Department of Defense, “DoD Cyber Strategy 2018” (articulating “defend forward” strategy); Derek B. Johnson, “DOJ official says ‘name and shame’ is one piece of the puzzle” (January 18, 2019); and staff, “US imposes sanctions on Russia over cyber-attacks,” BBC (April 16, 2021), <https://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html>, [https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER\\_STRATEGY\\_SUMMARY\\_FINAL.PDF](https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF), <https://few.com/articles/2019/01/18/demers-doj-cyber-shame.aspx>, <https://www.bbc.com/news/technology-56755484>.
35. COL Timothy M. McKenzie, “Is Cyber Deterrence Possible?” Air Force Research Institute Papers (January 2017), [https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/0/CPP\\_0004\\_MCKENZIE\\_CYBER\\_DETERRENCE.PDF](https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/0/CPP_0004_MCKENZIE_CYBER_DETERRENCE.PDF).
36. Zachary Cohen, Vivian Salama, & Brian Fung, “Concern mounts over government cyber agency’s struggle to respond to hack fallout,” CNN (January 2, 2021), <https://www.cnn.com/2021/01/02/politics/hack-goverment-cyber-struggle-respond-fallout/index.html>.
37. Maxim Kovalsky, Deputy CISO for NYC Cyber Command, “Overview of NYC Cyber Command,” ISSA-NOVA Chapter Meeting (September 23, 2021) (Roth attended online presentation).
38. Maggie Bruner, “Challenges and Opportunities in State and Local Cybercrime Enforcement,” *Journal of National Security Law & Policy*, Vol. 10:563, 572, 578.
39. Dr. Nic Butler, “The Pirate Hunting Expeditions of 1718,” Charleston County Public Library (November 23, 2018), <https://www.ccpl.org/charleston-time-machine/pirate-hunting-expeditions-1718>.
40. Ibid.
41. Ibid.
42. Ian Harvey, “Pirate Hunters risked their lives to bring the Golden Age of Piracy to a close,” *Vintage News* (February 9, 2017), <https://www.thevintagenews.com/2017/02/09/pirate-hunters-risked-their-lives-to-bring-the-golden-age-of-piracy-to-a-close/>.

## NOTES

43. Ensign Lucian Rombado, “Grant Cyber Letters of Marque to Manage Hack Backs,” U.S. Naval Institute (October 2019), <https://www.usni.org/magazines/proceedings/2019/october/grant-cyber-letters-marque-manage-hack-backs>.
44. William Young, “A Check on Faint-Hearted Presidents: Letters of Marque and Reprisal,” 66 *Wash. & Lee L. Rev* 897-898 (2009), <https://law2.wlu.edu/deptimages/Law%20Review/66-2Young.pdf>.
45. Frank Colon, “Letters of Marque for Private Sector Cyber Defense,” *Cybersecurity & Information Systems Information Analysis Center* (Vol. 7, Issue 4, Spring 2020), <https://csiac.org/articles/rebooting-letters-of-marque/>.
46. Rombado, “Grant Cyber Letters of Marque to Manage Hack Backs.”
47. See, for example, Jen Ellis, “Why hack back is still wack: 5 causes for concern,” *Security Magazine* (October 13, 2021), <https://www.securitymagazine.com/articles/96295-why-hack-back-is-still-wack-5-causes-for-concern>.
48. Staff, “How wild was the Wild West?” *History Extra*, BBC (July 1, 2019), <https://www.historyextra.com/period/victorian/wild-west-how-lawless-was-american-frontier/>.
49. Marshall Trimble, “The Train Robbers,” *True West Magazine* (November 2018), <https://truwestmagazine.com/article/the-train-robbers/>.
50. “Pinkerton, Allan,” *Encyclopedia.com* (May 29, 2018), <https://www.encyclopedia.com/people/social-sciences-and-law/crime-and-law-enforcement-biographies/allan-pinkerton>.
51. Staff, “How wild was the Wild West?” *History Extra*, BBC (July 1, 2019), <https://www.historyextra.com/period/victorian/wild-west-how-lawless-was-american-frontier/>.
52. “History,” *Railroad Police* (undated), <https://www.therailroadpolice.com/history>, <https://www.therailroadpolice.com/history>.
53. Staff, “How wild was the Wild West?” *History Extra*, BBC (July 1, 2019), <https://www.historyextra.com/period/victorian/wild-west-how-lawless-was-american-frontier/>.
54. *Ibid.*
55. “Pinkertons,” *Encyclopedia of Chicago* (undated), <http://www.encyclopedia.chicagohistory.org/pages/969.html>.
56. *Ibid.*
57. 49 U.S.C. § 24305(e) (codifying Railroad Passenger Services Act of 1970).
58. *Ibid.*; Paul Miller, “The Railroad Police – history” (undated), <http://www.therailroadpolice.com/history>.
59. US v. Tillman, E.D. La (Criminal Docket No 14-041) (circa February 18, 2014), DOJ memo noting that defendant was “Mirandized,” <https://www.justice.gov/file/339456/download>.
60. Staff, “Cybersecurity,” *Statista* (undated), <https://www.statista.com/outlook/tmo/cybersecurity/ united-states>.
61. Adm. Dennis C. Blair, Hon. Michael Chertoff, Frank J. Ciluffo, & Nuala O’Connor, “Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats,” Center for Cyber & Homeland Security, George Washington University (October 2016), <https://wayback.archive-it.org/5184/20190103002934/https://cchs.gwu.edu/sites/g/files/zaxdzs2371/ff/downloads/CCHS-ActiveDefenseReportFINAL.pdf>.
62. See, for example, Robert Barnes, “Supreme Court tightens, slightly, rules for police entering a home without a warrant,” *The Washington Post* (June 23, 2021); Public, “Hot Pursuit,” *Wikipedia* (undated), <https://www.cbjlawyers.com/decision-in-hot-pursuit-case-unlikely-to-have-significant-ramifications/>, [https://en.wikipedia.org/wiki/Hot\\_pursuit](https://en.wikipedia.org/wiki/Hot_pursuit).
63. Jessica Nicholson & Giulia McHenry, “Measuring Cross-Border Data Flows: Data, Literature, and Considerations,” Internet Policy Task Force, National Telecommunications and Information Administration, Department of Commerce (May 10, 2016), [https://www.ntia.doc.gov/files/ntia/publications/measuring\\_cross\\_border\\_data\\_flows\\_pre-roundtable\\_materials\\_2016\\_05\\_05v2.pdf](https://www.ntia.doc.gov/files/ntia/publications/measuring_cross_border_data_flows_pre-roundtable_materials_2016_05_05v2.pdf).
64. Homepage, Internet Policy Task Force, National Telecommunications and Information Administration, U.S. Department of Commerce (May 10, 2016), <https://www.ntia.doc.gov/category/internet-policy-task-force>.
65. Staff, “Country Case: Inherently governmental and critical functions in the United States”, OECD (undated), <https://www.oecd.org/governance/procurement/toolbox/search/inherently-governmental-critical-functions-united-states.pdf>.
66. See, for example, Peter Singer, “The Dark Truth about Blackwater,” *Brookings Institution* (October 2, 2007), <https://www.brookings.edu/articles/the-dark-truth-about-blackwater/>.
67. See Police Foundation, “Best Practices in Event Deconfliction,” *CALEA* (October 2016), 1, [https://www.calea.org/sites/default/files/2019-02/EventDeconfliction\\_PoliceFoundation.pdf](https://www.calea.org/sites/default/files/2019-02/EventDeconfliction_PoliceFoundation.pdf).

## NOTES

68. See, for example, Robert McMillan and Aruna Viswanatha, “North Korea Turning to Cryptocurrency Schemes in Global Heists, U.S. Says,” *The Wall Street Journal* (February 17, 2021), <https://www.wsj.com/articles/u-s-authorities-charge-north-koreans-in-long-running-hacking-scheme-11613581358>; but also see, Andy Greenberg, “North Korea Hacked Him. So He Took Down its Internet,” *Wired* (February 2, 2022), <https://www.wired.com/story/north-korea-hacker-internet-outage/>.
69. Staff, “Country Case: Inherently governmental and critical functions in the United States,” OECD (undated), <https://www.oecd.org/governance/procurement/toolbox/search/inherently-governmental-critical-functions-united-states.pdf>.
70. “An in-depth look at hacking back, active defense, and cyber letters of marque,” MalwareTech (November 7, 2021), <https://www.malwaretech.com/2021/11/an-in-depth-look-at-hacking-back-active-defense-and-cyber-letters-of-marque.html>
71. See, for example, Press Release, “Schengen Area – The Commission proposes to facilitate cross border surveillance and ‘hot pursuit’ between Member States”, European Council, European Union (July 19, 2005), [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_05\\_970](https://ec.europa.eu/commission/presscorner/detail/en/IP_05_970).
72. Gaia Pianigiani, “Italy Jails Ex-Officials for Rendition,” *The New York Times* (February 12, 2013), <https://www.nytimes.com/2013/02/13/world/europe/former-italian-military-officials-sentenced-in-abduction-of-abu-omar.html>.
73. Office of Counterintelligence (DXC), Defense CI & HUMINT Center, Defense Intelligence Agency, “Terms and Definitions of Interest for DoD Counterintelligence Professional,” at GL-129 (May 2, 2011).
74. Robert McMillan and Aruna Viswanatha, “North Korea Turning to Cryptocurrency Schemes in Global Heists, U.S. Says,” *The Wall Street Journal*, <https://www.wsj.com/articles/u-s-authorities-charge-north-koreans-in-long-running-hacking-scheme-11613581358>.
75. Andy Greenberg, “North Korea Hacked Him. So He Took Down its Internet,” *Wired* (February 2, 2022),
76. See, for example, Federal Acquisition Rules, Subpart 9.104-2, Special Standards:  
 “(a) When it is necessary for a particular acquisition or class of acquisitions, the contracting officer shall develop, with the assistance of appropriate specialists, special standards of responsibility,” [https://www.acquisition.gov/far/part-9#FAR\\_9\\_104\\_2](https://www.acquisition.gov/far/part-9#FAR_9_104_2)
77. Blair et al., “Into the Gray Zone,” 19.
78. *Ibid.*, 8-11.
79. This would include the use of payloads embedded in files on client networks that an intruder might steal and execute from the intruder’s machine.
80. Panayotis A. Yannakogeorgos, “Strategies for Resolving the Cyber Attribution Challenge,” 12, *Perspectives on Cyber Power*, Air Force Research Institute Papers (December 2013), describing compromised hosts used as cutouts as “botnets,” [https://media.defense.gov/2017/May/11/2001745613/-1/-1/0/CPP\\_0001\\_YANNAKOGEOGOS\\_CYBER\\_TTRIBUTION\\_CHALLENGE.PDF](https://media.defense.gov/2017/May/11/2001745613/-1/-1/0/CPP_0001_YANNAKOGEOGOS_CYBER_TTRIBUTION_CHALLENGE.PDF).
81. If the U.S. Department of Justice (DOJ) pursues a prosecution based on a CADTF licensee’s report, the CADTF licensee must be prepared to serve as a witness.



# Conceptualizing Cyberspace Security Diplomacy

---

The Honorable Christopher A. Ford

**A**t a time when crippling ransomware incidents<sup>[1]</sup> have drawn awareness to the risks of cyberattack as perhaps never before—and in which cyber criminals often enjoy toleration and a symbiotic relationship with the government in safe haven jurisdictions such as Russia<sup>[2]</sup>—cybersecurity and cyber defense are topics of critical importance. In response to these threats, government officials<sup>[3]</sup> and private cybersecurity experts<sup>[4]</sup> alike seek effective responses, which increasingly involves cybersecurity-focused diplomatic engagement. This article offers a tentative framework for conceptualizing this challenge and developing more systematic approaches for cybersecurity policy interventions that will support and facilitate cyber diplomacy.

## *The Advent of Cyberspace Security Diplomacy*

In their ongoing arms race with cyber criminals and state-sponsored cyber adversaries, the Western countries afflicted by such cyberattacks are working to find more effective approaches to combat the problem. Most efforts are technical in nature, relating to specific means to resist and counteract the tactics, techniques, and procedures (TTPs) used by cyber adversaries to exploit information systems, or to ways to hold them accountable through law enforcement or other means.



**The Hon. Christopher Ford** is Distinguished Policy Advisor at MITRE Labs and a Visiting Fellow at Stanford University's Hoover Institution. He previously served as U.S. Assistant Secretary of State for International Security and Nonproliferation, also performing the duties of the Under Secretary for Arms Control and International Security. The views expressed here are his personal opinions, and do not necessarily represent those of anyone else.

A less well known but growing component of the West's cyber defense, however, is also diplomatic, in the form of cyberspace security diplomacy. As exemplified by the U.S. State Department's Office of the Coordinator for Cyber Issues (CCI)<sup>5]</sup> this work involves engaging with foreign counterparts to develop and articulate common understandings of peacetime norms for cyber activity; this includes the principles set forth by United Nations experts in 2013 that states should not attack each other's civilian critical infrastructure in peacetime.<sup>6]</sup> It also involves promoting the adoption of common positions in attributing cyberattacks to malicious cyber actors and in imposing penalties (e.g., sanctions, public condemnation, or prosecution) upon those actors.

Cyberspace security diplomacy was responsible for a 2019 agreement reached by 28 Western countries expressing support for the "evolving framework of responsible state behavior in cyberspace," supporting "targeted cybersecurity capacity building to ensure that all responsible states can implement this framework and better protect their networks from significant disruptive, destructive, or otherwise destabilizing cyber activity," and pledging to "work together on a voluntary basis to hold states accountable when they act contrary to this framework."<sup>7]</sup> It is now not unusual for US officials to impose sanctions upon malicious cyber actors in other countries, nor for US law enforcement agencies to issue criminal indictments.<sup>8]</sup> Work by US diplomats, intelligence officials, and law enforcement officers to engage their international counterparts, moreover, has helped encourage foreign governments impose concrete international steps to penalize such malefactors as well.<sup>9]</sup>

In the US, such cyber-diplomacy has been undertaken under the aegis of the *2018 National Cyber Strategy*, which called for "an international Cyber Deterrence Initiative" that would include building "a coalition [of states] and develop[ing] tailored strategies to ensure

adversaries understand the consequences of their own malicious cyber behavior.”

The United States will work with like-minded states to coordinate and support each other’s responses to significant malicious cyber incidents, including through intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken, and joint imposition of consequences against malign actors.<sup>[10]</sup>

Such diplomacy cannot solve all today’s problems of rampant cybercrime and state-sponsored cyber assaults, of course, but it is a key piece of the puzzle as Western societies build effective responses.

Cyber diplomacy involves convincing others to agree upon cyber threat assessments, the attribution of specific attacks to specific actors, and what sorts of response may be appropriate in any given case. While there are extremely technical aspects of this work (such as the analysis of cyber-attackers’ TTPs and intelligence-derived information in connection with attribution assessments) cyber diplomacy is not only a technical matter but also a persuasive and even political exercise, in which international counterparts work to develop areas of agreement and decide upon courses of action. Because cyberspace security diplomacy is a relatively new field, though, little study has hitherto been done of the persuasive aspects of this work.

### *The Diplomacy of International Cyber-Collaboration*

Cyberspace security diplomacy revolves heavily around international efforts to come to agreement on cyber threats – and on the *attribution* of a cyber-attack to a particular malicious cyber actor. “Attribution diplomacy” is critical to the State Department’s cyberspace security engagements. Though the conventional wisdom used to hold that such attribution was all but impossible in cyberspace,

... [i]t actually is possible to do more by way of attribution than most observers once thought possible. It is sometimes even possible to share enough information with one’s friends and partners that they, too, can have a reasonable degree of confidence in the source of an attack.<sup>[11]</sup>

Attribution engagement opens possibilities “not just for more direct forms of response and deterrence, but indeed also for cyber diplomacy.”

... [W]e are getting better and better at mobilizing partners to condemn the condemnable ... In February 2020 [for instance], 20 individual states – and the European Union as a whole – also joined in condemning the disruptive cyber attack against the country of Georgia mounted in October 2019 by the Russian GRU military intelligence service.

In April 2020, moreover, the United States and several other likeminded countries issued concerted statements in response to an alert issued by the Czech Republic about its detection of impending cyber-attacks targeting its health sector, warning that such actions would result in consequences. This was the first time that likeminded states have come

together to warn against a specific *future* cyber-attack, and we believe our warning had an effect; despite preparatory work by the would-be perpetrators, no major cyber-attack ultimately occurred in that case.

Reinforced by the increasing imposition of not just United States but now also European Union sanctions in egregious cyber cases – coupled with “defend forward” activities [by the U.S. Department of Defense] – this cyberspace security diplomacy is helping to increase the costs and risks faced by the perpetrators of malicious cyber activity.<sup>[12]</sup>

Such diplomatic engagement in support of collaborative action among allies and partners against cyberspace threats is also a hallmark of Biden administration policy. In July 2021, for instance, President Biden announced that “[a]n unprecedented group of allies and partners,” including the European Union (EU), the United Kingdom (UK), and North Atlantic Treaty Organization (NATO), was “joining the United States in exposing and criticizing the PRC’s malicious cyber activities.”

Our allies and partners are a tremendous source of strength and a unique American advantage, and our collective approach to cyber threat information sharing, defense, and mitigation helps hold countries like China to account. Working collectively enhances and increases information sharing, including cyber threat intelligence and network defense information, with public and private stakeholders and expands diplomatic engagement to strengthen our collective cyber resilience and security cooperation. Today’s announcement builds on the progress made from the President’s first foreign trip. From the G7 and EU commitments around ransomware to NATO adopting a new cyber defense policy for the first time in seven years, the President is putting forward a common cyber approach with our allies and laying down clear expectations and markers on how responsible nations behave in cyberspace.<sup>[13]</sup>

In connection with this announcement, US officials announced the criminal indictment of four hackers from China’s Ministry of State Security (MSS) for their involvement in “a multiyear campaign targeting foreign governments and entities in key sectors, including maritime, aviation, defense, education, and healthcare in at least a dozen countries.”<sup>[14]</sup> Beyond these unilateral national measures, however, Biden administration officials declared that these international cyberspace security partners had agreed, for the first time as a group, to “share intelligence on cyberthreats and collaborate on network defenses and security.”<sup>[15]</sup> On the heels of the EU agreement to extend its legal framework for an additional year for imposing sanctions in response to cyberattacks, the Biden administration’s message in announcing the new group of international cybersecurity partners suggested that such collaborations are the wave of the future.<sup>[16]</sup>

### ***A Framework for Thinking About Threat Persuasion***

Naturally, the impact such collaborations will have upon the cost-benefit calculations of

those who engage in malicious cyber activity—particularly when such activity is sponsored by state-level actors—still remains to be seen. Because cyber-diplomacy is increasingly important, however, this article suggests a lens through which to think systematically about the processes of persuasive engagement between international partners and to help develop concepts for how specific policy interventions could facilitate such diplomacy.

Abstracting from the specifics of the cyber arena, one could imagine a basic framework for the dynamics of persuasive threat engagement—that is, of trying to persuade another actor, in a context highly dependent upon specialized technical information or intelligence collection, that a third party presents a threat or is responsible for a particular offense. Here, the likelihood of agreement will depend upon the interaction of three main variables: (1) the strength and reliability of the threat information available from the first party; (2) the degree of trust the second party places in the first party; and (3) the magnitude of the practical consequences or implications of reaching agreement.

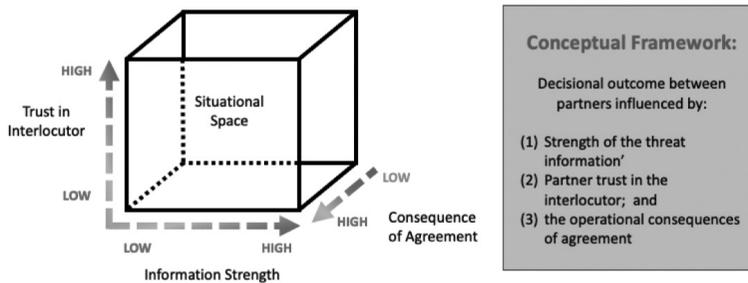


Figure 1. Situational Space

This situational space is represented in **Figure 1**. The reliability of the information is depicted along the X axis of the cube, from low strength on the left (*i.e.*, ambiguous technical assessments and/or low-confidence intelligence assessments) to high strength on the right (*i.e.*, compelling assessments and/or high-confidence information). The general level of trust the second party feels it can have in the honesty, integrity, and good faith of the first party is depicted along the Y axis, running from low trust (at the bottom) to high trust (at the top).

Finally, the consequences of agreement are depicted along the Z axis - running into the page, as it were, and making **Figure 1** into a three-dimensional graphic - from high to low. This consequences axes encodes the assumptions that agreeing upon the existence of a threat, or upon the fact that a given third party is indeed responsible for some bad act, will tend to put pressure upon the second party to take some course of action in response. To the degree that such a course of action would tend to impose greater risks or burdens upon the second party (*e.g.*, imposing sanctions upon a country likely to react harshly to such pressure), the consequence would be scored as high. To the degree that agreement would tend to lead to less costly or risky actions (*e.g.*, making verbal condemnations, or punishing a third party which would have few ways to retaliate), the consequence score would be rated as low.

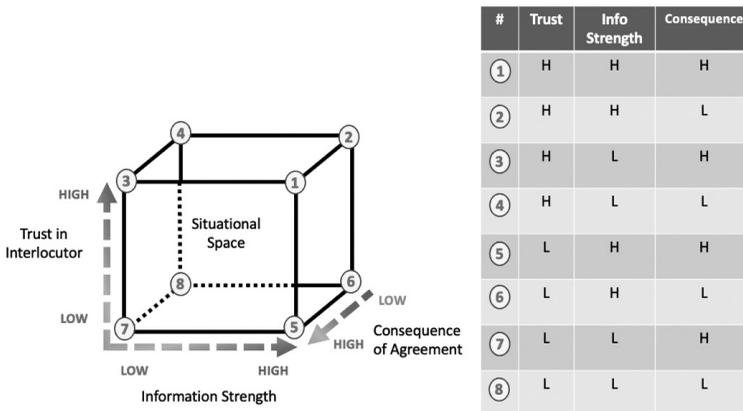


Figure 2. Situational Polar Cases

This graphic representation can be interpreted as shown in **Figure 2**. The table on the right sets out the eight polar cases that can be mapped three-dimensionally across the situational space of **Figure 1**. The various polar cases in the table are mapped onto the diagrammed cube on the left, defining the outer boundaries of situational possibilities. Graphically speaking, situations *in between* these hypothesized extremes of maximal or minimal information strength, trust, and consequence—e.g., “fairly strong” information, “some distrust,” or “moderate” or “uncertain” consequences—would appear inside the cube rather than on its outer limits.

The impact of these variables in terms of their presumed impact upon decisional outcomes is depicted graphically in **Figures 3, 4, and 5**, as follows:

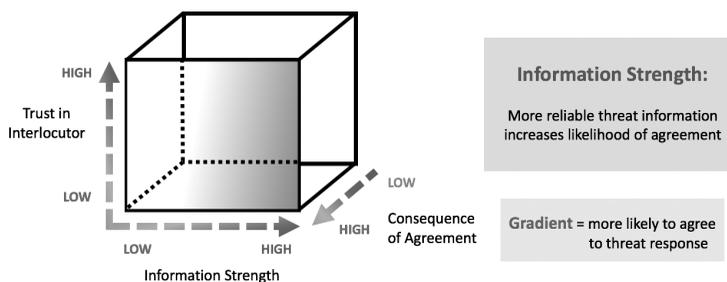


Figure 3. Likelihood of Agreement: Part I

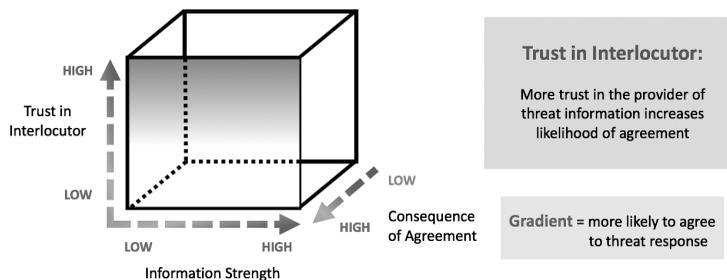


Figure 4. Likelihood of Agreement: Part II

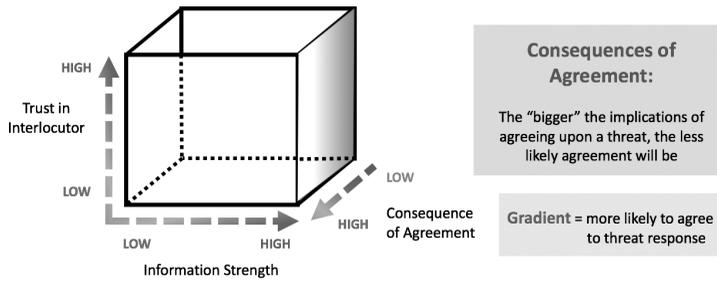


Figure 5. Likelihood of Agreement: Part III

These graphics may appear complicated, but the insights behind them are simple. One’s interlocutor will be maximally likely to agree when the information is highly reliable, when that interlocutor has a strong relationship of trust in the party making the request, and when the consequences of agreement are easily borne. Agreement is correspondingly less likely where information is weak, trust is low, and the likely operational consequences of such agreement are high.

Just how likely agreement is in any given case will depend upon where it is in the graphic space depicted by the situational cube created by the axes representing the degree to which reliable information is available, the *degree* to which the second party trusts the first, and the magnitude of the likely consequences of agreement. This is shown in **Figure 6**:

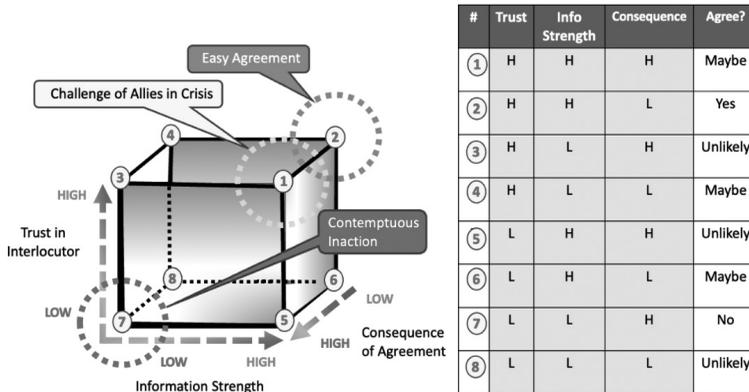


Figure 6. Likelihood of Agreement: Part IV

In **Figure 6**, the author has added his (subjective) assessments of likely decisional outcome to the tabular depiction on the right of the eight polar cases of **Figure 2**. In **Figure 6**, **Cases #7, #2, and #1** represent what may be particularly interesting examples. The first two of these are asymptotic decisional situations. In **Case #7**, the first party asks a great deal of the second (high consequences) but is not trusted by the second (low trust) and can only provide low-reliability information to support its case (low information strength). This is labeled contemptuous inaction, for that is very likely the reaction which such a demand would elicit.

In **Case #2**, by contrast, a trusted interlocutor provides solid information in support of its case, yet asks relatively little of the second party. Here, agreement would surely be all but inevitable.

A more challenging case is **Case #1**, in which a trusted interlocutor provides powerful information in support of its argument but asks a great deal of its interlocutor, thus setting the stage for a compelling but high-consequence decision. In **Figure 6**, this is labeled challenge of allies in crisis, for it suggests the kind of situation that might be faced by a close alliance responding to clear threats, but in ways that could lead to war. With sufficiently strong information and high trust, the parties might well agree, but it could be a difficult decision.

*Example of Threat Persuasion Conceptualized*

To try to put some real-world case studies into this framework, one might imagine the following potential examples:

- ◆ Afghanistan. After the terrorist attacks of September 11, 2001, the US felt it possessed very reliable information when it attributed those assaults to al-Qaeda. Washington thus turned to its NATO allies, with which it had a long and strong relationship of trust, asking them to participate in combat operations against the Taliban. Strong information and high trust produce strong scores along both the X and Y axes. The consequences for those allies, however, were arguably moderate, in the sense that they were being asked to go to war, but only against a low-technology enemy, in a theater where the US would clearly do most of the work, and in a context in which those allies would likely face terrorism at home anyway unless al-Qaeda were disrupted or defeated. The Afghanistan case might thus be depicted as **Point A** in **Figure 7**.

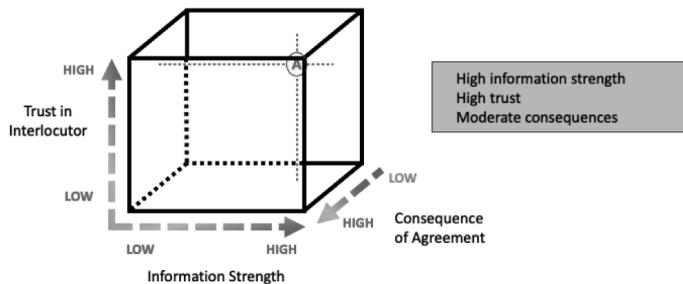


Figure 7. Thought Experiment: Afghanistan.

- ◆ **Iraq WMD.** Before the Iraq War of 2003, the US had what it and some of its most important and trusted allies felt was solid information on Iraqi weapons of mass destruction (WMD) threats. At the time, there was also a fairly high degree of trust on such matters among US allies.

The Iraq WMD case differs from Afghanistan, however, in that the perceived consequences of action were higher. At issue here was actually invading a country with a sizable military, and without UN Security Council “permission.” These implications

made action in Iraq much more fraught and challenging for US allies than taking action in Afghanistan, even before it became clear that the WMD intelligence information was gravely flawed. In this sense, the initial Iraq situation could arguably be situated at **Point B** in **Figure 8**, with both information reliability and allied trust declining over time toward **Point C**. (US officials were fortunate that their call for assistance occurred more toward the B end than the eventual C point of this progression.)

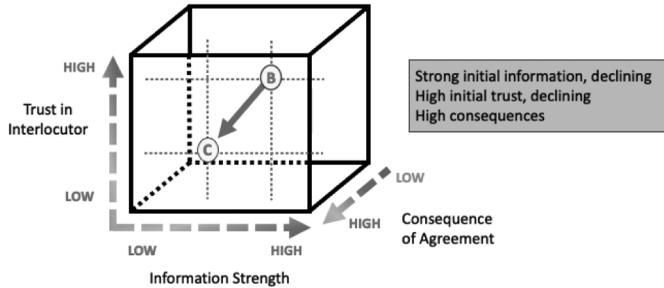


Figure 8. Thought Experiment: Iraq WMD.

- ◆ **Iran Nuclear Threats.** In dealing with Iran's clandestine nuclear program, the US had to contend with the legacy of distrust created by the Iraq WMD imbroglio in at least three respects. First, that historical baggage undermined confidence in WMD-related intelligence from unilateral national sources, particularly US ones. Second, it heightened allies' unease about US good faith. Third, it increased the perceived consequences of agreeing with Washington that Iran was trying to develop nuclear weaponry, by initially raising in some minds the specter of Iraq-style war if the US assessment of Iranian activity were accepted.

Partially counteracting these dynamics, however, was the role played by the IAEA as a third-party validator of at least some of the Iran nuclear threat information. This helped counteract some of the distrust of US information and good faith felt by other countries, since it was difficult to contest the IAEA's findings that Iran had been, at the very least, violating its safeguards obligations and engaging in exceedingly suspicious dual-use nuclear activity. (Eventually, in fact, the IAEA came to acquire significant information about Iran's nuclear weapons effort,<sup>[17]</sup> even before Israel exposed a huge archive of Iranian nuclear weapons program data to the world.<sup>[18]</sup>) As time went on, moreover, it became clearer—especially as the US became embroiled in the Iraqi insurgency—that a possible US invasion of Iran was not at issue after all, but rather merely a safeguards noncompliance finding by the IAEA and subsequent UN Security Council sanctions. Accordingly, the perceived significance of the Iran question moved along the Z-axis toward a lower consequences score. These shifts are shown in **Figure 9** as a movement between **Point D** and **Point E** within the situational cube; this arguably made possible the UN sanctions regime against Iran that was imposed beginning in 2006.

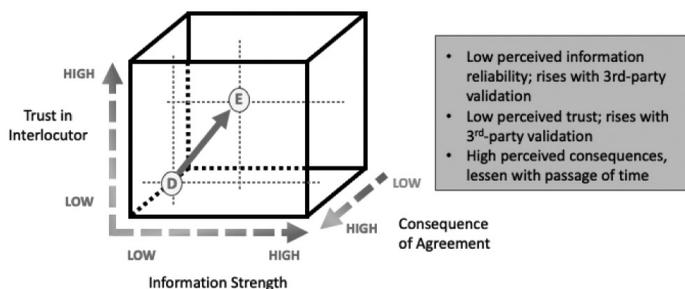


Figure 9. Thought Experiment: Iran Nuclear Threats.

◆ **Russia’s INF Violation.** A more recent case can be found in the US attempt to persuade its allies of Russia’s violation of the Intermediate-range Nuclear Forces (INF) Treaty. The US found Russia to be in noncompliance with INF in 2014, but it took years to bring NATO partners on board. Part of the difficulty related to the information in question. From a US perspective, the intelligence was strong, but it relied in part upon sources and methods that the US could not share with most NATO partners. The UK was the first to agree, as it benefits from “Five Eyes” intelligence-sharing. France and Germany, however, held back for longer, partly because they did not have access to as compelling a collection of intelligence, and partly because the perceived political consequences of agreeing on Moscow’s violation were uncomfortably high with the likely collapse of an arms control agreement. These challenges for Paris and Berlin became more acute with the election of President Donald Trump, whom they distrusted on a personal basis even on top of their political desire to avoid giving a victory to the US arms control hawks who viewed Russia’s development of INF-class missiles as a material breach of the Treaty.

The US turned things around and won allied agreement, however, for at least three reasons. First, it was able to share more intelligence with France and Germany, and walked their experts through some of the analysis that had contributed to the US conclusion. This shifted things along the information reliability axis. Second, irrespective of precisely how far the missile in question could be shown to have been flight-tested, it became increasingly clear that Russia was moving forward with production and deployment, and this was coming to present a significant new threat to NATO. This shifted things along the consequences axis since, as politically distasteful as the collapse of an arms control treaty was to European sensibilities, there was no way to avoid Russian INF-class threats no matter what NATO agreed.

Third, US allies came to realize that Washington would pull out of the INF Treaty in response to these threats irrespective of whether its partners agreed upon the Russian violation. These last two factors had the effect of shifting the situation significantly along the consequences axis, demonstrating that in light of Russia’s actions there was no way to save

the Treaty. (These developments also suggested there might be a real cost to NATO if this issue were to split the Alliance just as new Russian nuclear missiles came into service.) This increase in information strength and lessening of the perceived consequences of agreement can be seen in **Figure 10**, in the movement between **Point F** and **Point G**, and led to NATO's unanimous decision that Russia was in material breach of the Treaty.<sup>[19]</sup>

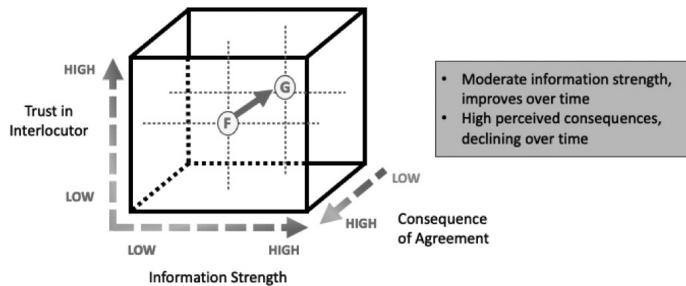


Figure 10. Thought Experiment: Russia's INF Violation.

- ◆ **Huawei in Britain.** One thought experiment related directly to cyberspace diplomacy is the UK's decision to ban products from the Chinese company Huawei in the UK's fifth generation (5G) telecommunications networks. Britain had been the first European country to offer Huawei a foothold in its networks,<sup>[20]</sup> but Huawei's increasing penetration of the British 5G market was a significant concern of US officials, who worried that the Chinese government might use Huawei and its equipment for malign purposes, and that Beijing's control over UK networks would provide it strategic leverage against this longstanding US intelligence-sharing and security partner.

Officials in London had been reassured by their own experts that they could mitigate the risk, but US officials disagreed, and pressed their counterparts to end reliance upon Huawei. At the State Department, for instance, officials pointed out the dangers of allowing a company subject to control by the Chinese Communist Party (CCP) to manage the UK's emerging 5G economy, the moral problems of subsidizing Huawei's ongoing work in facilitating human rights abuses in Xinjiang, and the risks of espionage or other malicious cyber activities. They also noted that, even by their own admission, British government experts had failed to mitigate technical risks associated even with Huawei's fourth-generation technology, and that mitigation in 5G would be impossible.<sup>[21]</sup> In early 2020, the US stepped up the pressure, sending a high-level delegation to London to present "a new dossier of intelligence challenging the UK's claim that it would be able to mitigate the risks of adopting Huawei technology in its 5G network." (One of these officials reportedly said that adopting technology from Huawei would be "nothing short of madness.")<sup>[22]</sup> Raising the ante further, another US official reportedly warned London that "Donald Trump is watching [this decision] closely," while a third observed that "Congress has made it clear they will want an evaluation of our intelligence sharing" with the UK if China were permitted control over British 5G networks.<sup>[23]</sup>

UK officials downplayed this threat to “Five Eyes” intelligence-sharing,<sup>[24]</sup> but US officials up to the level of Secretary of State Pompeo had indeed speculated about this possibility for months after the US had banned Huawei from its own networks.<sup>[25]</sup> In early 2020, the issue acquired an increasingly public profile in the UK, particularly as parliamentarians called for inquiries into Huawei risks.<sup>[26]</sup> Meanwhile, the Chinese government was lobbying in Huawei’s favor, even as press accounts revealed that Beijing had threatened trade retaliation against the Faroe Islands if Huawei did not get the 5G contract there.<sup>[27]</sup> Huawei itself also spent lavishly to win British favor, such as in donating to a charity founded by Prince Charles<sup>[28]</sup> and offering \$1.25 billion for a new research institute at Cambridge University.<sup>[29]</sup>

A few weeks after the US delegation’s visit, the UK announced that Huawei would continue to be permitted to build British 5G networks, but would be kept out of core parts of the system and would not be permitted to install equipment in or near particularly sensitive locations or facilities.<sup>[30]</sup> This British move was depicted as a defeat for the US,<sup>[31]</sup> but the UK revised its Huawei plans in July 2020, banning purchases of new Huawei 5G equipment after the end of the year, and also decreeing that existing Huawei equipment needed to be removed from UK networks by 2027.<sup>[32]</sup> UK officials then told telecommunications providers that they must stop installing Huawei equipment beginning in September 2021, and called for the “complete removal of high-risk vendors” from British 5G networks.<sup>[33]</sup>

From the outside, it is difficult to assess the specific reasons for the shifts in UK policy against Huawei during 2020. The intelligence information about Huawei reportedly provided to British officials by the US delegation may have had some impact, though it is unlikely that this proved decisive, since the initial decision to permit Huawei to control up to 35 percent of UK 5G networks was made after receiving the information in question.<sup>[34]</sup> Press reports have suggested that several additional factors likely played a role. Pressure had already been growing on the Johnson government within the Conservative Party, but this increased with the Chinese government’s crackdown on pro-democracy demonstrators and civil society in Hong Kong, as Beijing began moving in 2020 to destroy the “one-country, two-systems” dispensation it had long promised would protect freedoms there. (In widely televised violence, Hong Kong police had been cracking down on pro-democracy demonstrators since mid-2019,<sup>[35]</sup> and in June 2020, Chinese authorities forced upon Hong Kong a harsh new law against “subversion.”<sup>[36]</sup>) These developments highlighted the danger presented by the nature of the Chinese regime the Johnson government had initially been willing to give more than a one-third role in the UK digital economy. They also drew attention to the seeming ease with which Beijing could twist nominally independent Chinese entities (the supposedly independently elected government of Hong Kong, but also implicitly essentially any Chinese company, including Huawei) into instruments of CCP coercive power.<sup>[37]</sup>

In addition, the US announced additional moves against Huawei in the spring of 2020 that tended to “throw Huawei’s supply chain into chaos”<sup>[38]</sup> and made 5G reliance upon it

more difficult to sustain. Specifically, the US government imposed new limits on the use of US-made semiconductor design tools in making chips destined for Huawei. Since US-origin design software dominated the high end of the chip manufacturing market, this cut off a crucial source of Huawei technology,<sup>[39]</sup> as US export control officials would treat Huawei-designated transfers with a presumption of denial.<sup>[40]</sup> This helped lead the UK to conclude that it would have increasing difficulty in relying upon Huawei for 5G technology, thus making agreement to US demands seem less costly. “American sanctions” against Huawei, claimed one former UK diplomat, “left the UK with little choice.”<sup>[41]</sup>

These shifts changed the UK government’s perception of the relative consequences of agreeing to the US request for a Huawei ban, since the political impact of not agreeing was clearly rising because of CCP brutality in Hong Kong, even as the UK’s ability to reap the anticipated economic benefits of continued access to low-cost Huawei equipment was being called into question by tightening US export control rules. Accordingly, the Johnson government’s response adjusted. According to one government minister, “[a]s facts have changed, so has our approach.”<sup>[42]</sup> The Huawei case may be seen in the shift from **Point H to Point I** in **Figure 11**. As depicted there, a small increase is depicted in the information strength, and a more significant shift in terms of a reduction in the perceived consequences (*i.e.*, political and economic cost) of agreement.

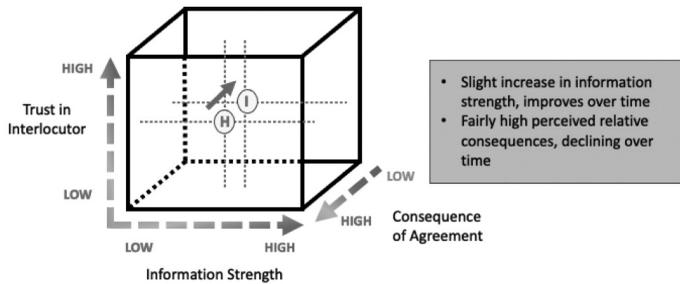


Figure 11. Thought Experiment: Huawei in Britain.

### Implications for Policy Interventions

Whether or not one agrees with this author’s assessments of outcome probabilities in **Figure 6** (or with his characterization of the aforementioned historical examples), this three-dimensional framework for understanding the interplay of information reliability, trust, and consequence may be useful in structuring how to think about developing and implementing policy interventions to increase the odds of success in threat engagement diplomacy. Such a conceptualization may be especially useful as the US steps up its cyberspace security diplomacy, as this framework may help point the way toward interventions specifically intended to boost information strength (X-axis), strengthen interlocutor trust (Y-axis), and/or lessen the perceived consequences of agreement (Z-axis) in order to drive situations more in the direction of the

decisional-outcome “sweet spot” depicted graphically below – that is, to push situations toward the zone of situational outcomes most conducive to agreement, as shown in **Figure 12** as a portion of the spherical zone around **Case #2** (easy agreement).

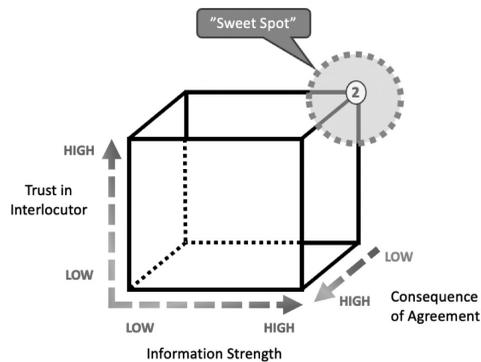


Figure 12. Desired End State of Agreement.

In the cyberspace context—in which diplomatic engagements often center around attribution diplomacy—such policy interventions could take various forms, including at least the following:

- I. Improved information sharing** is a way to help drive situations rightward along the information strength (X) axis in ways that would, all other things being equal, create a greater likelihood of agreement. This could mean doing more to share with international partners intelligence reporting that supports attribution analysis, either passing it directly to partners with whom one has good cyber-intelligence relationships (*e.g.*, within the “Five Eyes” partnership) or by downgrading information to be shared with others. Information sharing can also occur via public criminal indictments—which must meet due process standards and ultimately survive beyond a reasonable doubt proof standards for conviction if they get to court—or perhaps in connection with the imposition of sanctions.<sup>[43]</sup>

Whatever the means, however, building more effective mechanisms for secure sharing of attribution-relevant information would probably have the effect of making attribution agreement more likely. It can also help strengthen interlocutors’ perceptions of trust in the sharer, potentially causing agreement-conducive movement along the graphical Y-axis as well. (A country sharing more information with a second-party partner that is more trusted by the third-party target of diplomatic suasion than is the first country can also help spur movement along both axes: it enables the recipient of this information to leverage its own relationship of trust with the ultimate target.) Augmented information sharing can thus result in movement within the cubic situational space along both the X and Y axes, as depicted in **Case I** in **Figure 13**.

To the degree that attribution-relevant information can be shared publicly, or at least very widely within the broad open-source cybersecurity community, one might expect this to also support more positive outcomes in attribution diplomacy. The MITRE Corporation’s

“ATT&CK Matrix,” for instance, compiles and displays information about known malicious cyber activity TTPs for cybersecurity professionals on an open-source basis,<sup>[44]</sup> providing a resource for cybersecurity officials around the world whose job it is to defend against such attacks. In cases where private sector or governmental attribution assessments have been made about specific intrusions, however, it might be possible in the future to include not just information about specific TTPs themselves but also an indication of which bad actor originated a given technique and with whom that technique’s use is most frequently associated. To the degree that subsequent attribution diplomacy relies upon analysis of cyber-attack techniques, such a public record of past associations between bad actors and specific TTPs could help increase the credibility of subsequent attribution assessments, strengthening diplomatic persuasiveness.<sup>[45]</sup>

**II. Third-Party Validation** can also play an important role in increasing both information strength and interlocutor trust. In the cyber context, the third-party validation role is often played by private-sector cybersecurity firms who, in the wake of major incidents, often make public attribution assessments that can complement and reinforce those made by governments. Such validation can move things in agreement-friendly directions along both the X and Y axes of our situational graph, by augmenting the strength of information available for cyber-diplomatic persuasion and increasing the trust others can have. Working to strengthen interactions and engagements with a diverse range of private sector cybersecurity firms can be a way for government cyber-diplomats to increase the traction they will have with foreign counterparts. This is suggested graphically by **Case II** in **Figure 13**.

**III. Risk Mitigation** is another approach that could be used to increase the likelihood of positive decisional outcomes. This could include cyberspace-related capacity-building programming, analogous to the money the US spends through the State and Defense Departments to augment partner countries’ ability to support nonproliferation-related objectives.<sup>[46]</sup> The US already does some cyber-related capacity-building programming<sup>[47]</sup> – to which, incidentally, the MITRE Corporation has made important contributions, both directly for the US and in working with 10 sponsor countries in East Asia<sup>[48]</sup> – but it probably should do more, especially as it builds out its cyber diplomacy capabilities.<sup>[49]</sup> Such capacity-building efforts could focus in particular upon measures designed to support attribution diplomacy, such as improving partner countries’ own cyber collection and analytical capabilities (improving information strength), strengthening relationships between US and partner country cyber-related institutions (increasing trust), and improving partner incident response and cyber-systemic resilience (reducing the consequences of joint attribution decisions by helping better protect partners from cyber retribution). Through this prism, capacity-building programming could produce agreement-conducive movement along all three axes in the graphic representation, as shown by **Case III** in **Figure 13**.

IV. Over time, the US ability to build up a **Track Record of Accuracy** and a history of collaborative attribution decisions with its cybersecurity partners will also contribute to success in cyberspace security diplomacy. As noted, this is a new arena, since the conventional wisdom held that cyber attribution was essentially impossible. US officials are gradually building a record of engagement and collaboration on cyber attribution that is robbing the field of its initial strangeness, increasing relationships of trust, habituating foreign counterparts to attribution-focused engagement, and demonstrating that attribution is sometimes possible after all. This can hopefully create something of a virtuous circle of accelerating diplomatic success. This augmented trust is depicted graphically by Case IV in Figure 13 below.

V. **Improved Information Collection** is a final way to improve the odds of cyber-diplomatic agreement. With better intelligence information that supplements technical analysis of cyber-adversary TTPs, better analysis in understanding and drawing inferences from such TTPs and their patterns of employment, and other sources of relevant information, improved knowledge is likely to produce movement to the right along the Information Strength (X) axis, as shown by **Case V** in **Figure 13**.

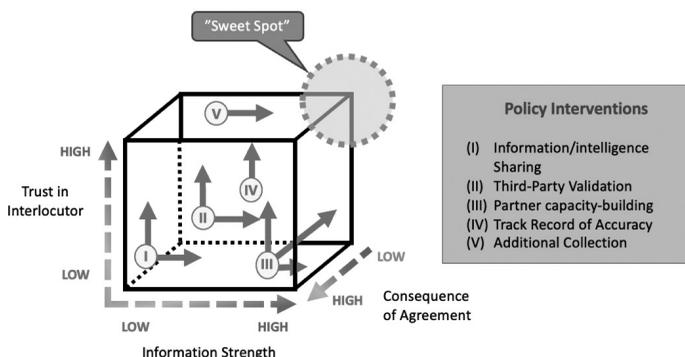


Figure 13. Policy Interventions.

## CONCLUSION

This article is not intended to provide a comprehensive list of the ways in which policy interventions could improve the prospects for successful cyberspace security diplomacy. It has tried, however, to provide an intellectual framework for thinking about this problem, and to sketch out the key variables—information strength, partner trust, and operational consequence—that affect the likelihood of success in attribution diplomacy. This framework can help policy analysts and decision-makers focus more effectively on how to improve the ways in which our nation responds to cyberspace threats.🛡️

## NOTES

1. Collin Eaton and Dustin Volz, “Colonial Pipeline CEO Tells Why He Paid Hackers \$4.4 Million Ransom,” *The Wall Street Journal* (May 19, 2021), <https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636>; Julie Creswell, Nicole Perloth, and Noam Scheiber, “Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business,” *The New York Times* (June 3, 2021), <https://www.nytimes.com/2021/06/01/business/meat-plant-cyberattack-jbs.html>.
2. Ellen Nakashima, Hamza Shaban, & Rachel Lerman, “The Biden administration seeks to rally allies and the private sector against the ransomware threat,” *The Washington Post* (June 4, 2021) (quoting senior Biden administration official that “countries like Russia ignore their activities as long as they don’t target companies, people or government agencies inside their borders”), <https://www.washingtonpost.com/business/2021/06/04/white-house-fbi-ransomware-attacks/>; U.S. Department of the Treasury, “Treasury Sanctions Russia with Sweeping New Sanctions Authority” (April 15, 2021) (noting that the Russian Security Service [FSB] “cultivates and co-opts criminal hackers ... enabling them to engage in disruptive ransomware attacks and phishing campaigns”), <https://home.treasury.gov/news/press-releases/jy0127>.
3. Brian Fung, Geneva Sands, Rachel Janfaza, and Zachary Cohen, “FBI director sees ‘parallels’ between challenge posed by ransomware attacks and 9/11,” *CNN* (June 4, 2021) (noting that there is “a developing consensus within the Biden administration that ransomware ranks among the gravest threats to national security the United States has ever faced”), <https://www.cnn.com/2021/06/04/politics/christopher-wray-cyberattacks-9-11/index.html>.
4. Brenda R. Sharton, “Ransomware Attacks Are Spiking. Is Your Company Prepared?” *Harvard Business Review* (May 20, 2021), <https://hbr.org/2021/05/ransomware-attacks-are-spiking-is-your-company-prepared>.
5. U.S. Department of State, Office of the Coordinator for Cyber Issues website, <https://www.state.gov/bureaus-offices/secretary-of-state/office-of-the-coordinator-for-cyber-issues/>.
6. “Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,” United Nations report A/70/174 (July 22, 2015), at 8, ¶ 13(f) (noting that states should not “conduct or knowingly support [cyber] activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public”), [https://www.un.org/ga/search/view\\_doc.asp?symbol=A/70/174](https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174).
7. Joint Statement on Advancing Responsible State Behavior in Cyberspace (September 23, 2019), <https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/>. The Joint Statement was signed by Australia, Belgium, Canada, Colombia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Japan, Latvia, Lithuania, the Netherlands, New Zealand, Norway, Poland, the Republic of Korea, Romania, Slovakia, Slovenia, Spain, Sweden, the United Kingdom, and the United States.
8. David E. Sanger and Andrew E. Kramer, “U.S. Imposes Stiff Sanctions on Russia, Blaming It for Major Hacking Operation,” *The New York Times* (April 15, 2021), <https://www.nytimes.com/2021/04/15/world/europe/us-russia-sanctions.html>; U.S. Department of Justice, “U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations” (October 4, 2018), <https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and>; U.S. Department of Justice, “Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information” (December 20, 2018).
9. Lorne Cook, “First-ever EU cyber sanctions hit Russians, Chinese, NKoreans,” *Associated Press* (July 30, 2020), <https://apnews.com/article/malware-technology-foreign-policy-international-news-military-intelligence-978f1494313a545e6e7e568e5f9782bf>; Laurens Cerulus, “EU countries extend sanctions against Russian, Chinese hackers,” *Politico* (May 17, 2021), <https://www.politico.eu/article/eu-council-cyber-sanctions-russia-china-hackers/>.
10. *National Cyber Strategy of the United States of America* (September 2018), 21, <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.
11. Assistant Secretary of State Christopher Ford, “International Security in Cyberspace: New Models for Reducing Risk,” *Arms Control and International Security Papers*, vol. I, no. 20 (October 20, 2020), 7, <https://irp-cdn.multiscreensite.com/ce29b4c3/files/uploaded/ACIS%20Paper%2020%20-%20Cyberspace.pdf>.
12. *Ibid.*
13. The White House, “The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People’s Republic of China,” press release (July 19, 2021), <https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/>.

NOTES

14. “The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity,” *supra*.
15. Christina Wilkie, “U.S., NATO and EU to blame China for cyberattack on Microsoft Exchange Servers” (July 19, 2021), paraphrasing Biden administration official, <https://www.cnn.com/2021/07/19/nato-and-eu-launch-a-cyber-security-alliance-to-confront-chinese-cyberattacks.html>.
16. Ionut Arghire, “European Union Extends Framework for Cyberattack Sanctions” (May 18, 2021), <https://www.security-week.com/european-union-extends-framework-cyberattack-sanctions>.
17. IAEA, “Implementation of the NPT Safeguards Agreement and Relevant Provisions of Security Council Resolutions in the Islamic Republic of Iran,” GOV/2011/65 (November 8, 2011), <https://www.iaea.org/sites/default/files/gov2011-65.pdf>.
18. David E. Sanger and Ronen Bergman, “How Israel, in Dark of Night, Torched Its Way to Iran’s Nuclear Secrets,” *The New York Times* (July 15, 2018), <https://www.nytimes.com/2018/07/15/us/politics/iran-israel-mossad-nuclear.html>.
19. Jim Garamone, “NATO Agrees: Russia in Material Breach of INF Treaty,” *Defense.gov* (December 5, 2018), <https://www.defense.gov/Explore/News/Article/Article/1705843/nato-agrees-russia-in-material-breach-of-inf-treaty/>.
20. Adam Satariano, Stephen Castle, and David E. Sanger, “U.K. Bars Huawei for 5G as Tech Battle Between China and the West Escalates,” *The New York Times* (July 14, 2020), <https://www.nytimes.com/2020/07/14/business/huawei-uk-5g.html>.
21. Assistant Secretary of State Christopher Ford, “Huawei and Its Siblings, the Chinese Tech Giants: National Security and Foreign Policy Implications,” remarks to the Multilateral Action on Sensitive Technology (MAST) Plenary Meeting in Washington, DC (September 11, 2019), <https://www.newparadigmsforum.com/p2431>.
22. Helen Warrell, “U.S. presses Boris Johnson with new dossier on Huawei security risks,” *Financial Times* (January 13, 2020), <https://www.ft.com/content/1d7f44b4-3643-11ea-a6d3-9a26f8c3c3ba4>; Dan Sabbagh, “Using Huawei in UK 5G networks would be ‘madness,’ US says,” *The Guardian* (January 13, 2020), <https://www.theguardian.com/technology/2020/jan/13/using-huawei-in-uk-5g-networks-would-be-madness-us-says>. (By way of full disclosure, the author of this article was one of the officials on that U.S. delegation.)
23. Warrell, *supra*; Sabbagh, “Using Huawei in UK 5g networks,” *supra*.
24. Dan Sabbagh, “US intelligence sharing will not be jeopardized if UK uses Huawei – MIS head,” *The Guardian* (January 12, 2020), <https://www.theguardian.com/technology/2020/jan/12/huawei-technology-poses-no-threat-to-uk-security-ex-mis-head>.
25. Cecelia Kang and David E. Sanger, “Huawei Is a Target as Trump Moves to Ban Foreign Telecom Gear,” *The New York Times* (May 15, 2019), <https://www.nytimes.com/2019/05/15/business/huawei-ban-trump.html>.
26. “Using Huawei in UK 5G network ‘madness,’ says US,” *BBC News* (January 14, 2020), <https://www.bbc.com/news/business-51097474>.
27. Adam Satariano, “At the Edge of the World, a New Battleground for the U.S. and China,” *The New York Times* (December 20, 2019), <https://www.nytimes.com/2019/12/20/technology/faroe-islands-huawei-china-us.html>.
28. Satariano, Castle, and Sanger, *supra*.
29. Huawei, “Huawei to Build an Optoelectronics R&D and Manufacturing Centre in Cambridge” (June 25, 2020), <https://www.huawei.com/en/news/2020/6/huawei-optoelectronics-rd-manufacturing-centre-cambridge>.
30. Adam Satariano, “Britain Defies Trump Plea to Ban Huawei from 5G Network,” *The New York Times* (January 28, 2020), <https://www.nytimes.com/2020/01/28/technology/britain-huawei-5G.html>.
31. Satariano, “Britain Defies Trump Plea,” *supra*.
32. Leo Kelion, “Huawei 5G kit must be removed from UK by 2027,” *BBC News* (July 14, 2020), <https://www.bbc.com/news/technology-53403793>; Satariano, Castle, and Sanger, *supra*.
33. “Huawei ban: UK to impose early end to use of new 5G kit,” *BBC News* (November 30, 2020), <https://www.bbc.com/news/business-55124236>; “Britain bans new Huawei 5G kit installation from September 2021,” Reuters (November 29, 2020), <https://www.reuters.com/article/us-britain-huawei/britain-bans-nw-huawei-5g-kit-installation-from-september-2021-idUSKBN28A005>.
34. Satariano, “Britain Defies Trump Plea,” *supra*.
35. Austin Ramzy and Mike Ives, “Hong Kong Protests, One Year Later,” *The New York Times* (June 9, 2020), <https://www.nytimes.com/2020/06/09/world/asia/hong-kong-protests-one-year-later.html>.

**NOTES**

36. “Hong Kong security law: what is it and is it worrying?” BBC News (June 30, 2020), <https://www.bbc.com/news/world-asia-china-52765838>.
37. Quoted by Satariano, Castle, and Sanger, *supra*.
38. Satariano, Castle, and Sanger, *supra*.
39. Assistant Secretary of State Christopher Ford, “U.S. National Security Export Controls and Huawei,” Arms Control and International Security Papers, vol. 1, no. 8 (May 20, 2020), 7, <https://irp-cdn.multiscreensite.com/ce29b4c3/files/uploaded/ACIS%20Paper%208%20-%20Export%20Controls%20and%20Huawei.pdf>.
40. Ana Swanson, “U.S. Delivers Another Blow to Huawei With New Tech Restrictions,” The New York Times (May 15, 2020), <https://www.nytimes.com/2020/05/15/business/economy/commerce-department-huawei.html>.
41. Satariano, Castle, and Sanger, *supra* (quoting unnamed former official who previously “represented the country’s interests in Silicon Valley”).
42. *Ibid.*, quoting Telecommunications Minister Oliver Dowden.
43. In US practice, however, the evidentiary standards for sanctions are generally lower; nor do officials generally have to make public the evidence upon which they rely in making sanctions determinations.
44. MITRE Corporation, “ATT&CK Matrix for Enterprise,” accessed on July 5, 2021, <https://attack.mitre.org/#>.
45. The ATT&CK Matrix does not currently or systematically include such notations, though it does occasionally indicate that particular hacker groups have employed particular techniques. MITRE Corporation, “Procedure Examples,” accessed on July 5, 2021 (noting that the “APT28,” “Sandworm,” and “Volatile Cedar” groups have employed the “vulnerability scanning” technique coded with the identification number T1595.002), <https://attack.mitre.org/techniques/T1595/002/>.
46. Assistant Secretary of State Christopher Ford, “Reforming Nonproliferation Programming,” remarks at the Stimson Center (September 25, 2018), <https://2017-2021.state.gov/remarks-and-releases-bureau-of-international-security-and-non-proliferation/reforming-nonproliferation-programming/index.html>; Assistant Secretary of State Christopher Ford, “The Evolution of International Security Capacity Building,” remarks to the CRDF Global Board of Directors (November 20, 2020), <https://2017-2021.state.gov/the-evolution-of-international-security-capacity-building/index.html>.
47. Kathryn Fitrell, “Office of the Coordinator for Cyber Issues: Leading and building effective international cyber diplomacy,” *State Magazine* (February 2021), <https://statemag.lab.prod.getusinfo.com/2021/02/0221office/>.
48. MITRE Corporation, “MITRE Strengthens Cyber Capacity of Developing Nations” (December 2019), <https://www.mitre.org/publications/project-stories/mitre-strengthens-cyber-capacity-of-developing-nations>.
49. U.S. Department of State, “Secretary Pompeo Approves New Cyberspace Security and Emerging Technologies Bureau” (January 7, 2021), <https://2017-2021.state.gov/secretary-pompeo-approves-new-cyberspace-security-and-emerging-technologies-bureau/index.html>.



# THE CYBER DEFENSE REVIEW

◆ PROFESSIONAL COMMENTARY ◆



# America's Cyber Auxiliary: Building Capacity and Future Operators

---

Lieutenant Colonel (Ret.) Jeffrey J. Fair

## **ABSTRACT**

*As the proliferation of cyber threats continues and the complexity and number of online systems grows, the need for updated cyber defenses to appropriately combat the threat will continue to expand into the future. The public and private sectors both heavily rely on accessing and using secure networks. The requirements for defense already outstrip the current capacity the US government has and needs reinforcement.*

*A cyber auxiliary can provide several ways to augment our cyber defense capacity. Education programs can equip the population with skills and awareness to serve as a solid front-line defense. A cadet program could enhance the educational approach and expose a larger population to in-depth knowledge of cyber defense and network operations, building a cadre for the future. Adult auxiliary members can add capacity to current cyber-defense organizations and be critical actors in aiding civil defense and even DoD. Much like the change in warfare observed during and after World War I, cyberspace is changing and growing. It is time to recognize both the environmental shifts and the opportunities available to the nation to get ahead of the coming cyber tsunami.*



**Jeff Fair** is the Vice President of Cybersecurity and Economic Development for the San Antonio Chamber of Commerce and as the lead for Cybersecurity San Antonio, a public-private partnership between the Chamber and the City of San Antonio charged with enhancing the cybersecurity industry in the city. Fair is a Ph.D. candidate at the George Washington University's Trachtenberg School of Public Policy and Administration.

His dissertation research includes governmental transparency in the U.S. Intelligence Community. He retired as a LTC after a 22-year career in the U.S. Army where he served in several organizations including the National Security Agency and U.S. Cyber Command. Fair holds a BA from George Washington University's Elliott School of International Affairs, an MBA from Hawaii Pacific University, a MPA from the University of Washington's Evans School, and a MSSI from the National Intelligence University (NIU). He later served as an adjunct for NIU, teaching courses at its NSA Academic Center.

**M**alicious cyber actors pose one of the greatest contemporary threats to the United States, but the country continues to fall well short of the capability and capacity needed to adequately protect itself in real-time. Cyber-attacks in the public and private sectors feature regularly in news reports, while increased post-attack mitigation efforts can aim only at limiting the damage. America and its allies even contend with threats to electoral systems and their democratic way of life as adversaries manipulate social media and other information flows. The threats are continuous, innumerable, and widespread, and the US is struggling to keep pace and identify better ways to defend against them.

As the number of government, military, and private cyber activities increases, the threat continues to grow and evolve. Several initiatives have been aimed at increasing US capacity in cyberspace. The federal government elevated U.S. Cyber Command (USCYBERCOM) to full combatant command status, expanding its purview and power structure. The move was joined by the military services, which initiated a rapid expansion of their own cyber units and specialists. The Trump administration adopted a new approach to dealing with malign cyber actors called persistent engagement, bringing a more active defense to bear on cyber threats that the Biden administration has decided to continue to practice. The involvement of USCYBERCOM in the pursuit of ransomware actors marks a new turn in the fight against threats that targets private sector companies, non-profits, school systems, and other government organizations at all levels.

The threat, however, remains real and continues to adversely affect organizations in all sectors: public, private, and non-profit. Some estimates show cyber-related crime and industrial espionage cost the US economy over \$2.1 trillion between 2015 and 2019.<sup>[1]</sup> Several high-risk sectors like health care, financial services, and manufacturing have been heavily targeted.

Not only will additional threats emerge over time, but an explosion in the number of online devices is adding more opportunities for malicious cyber actors. As government continues to invest in defense, so does the private sector, but the losses continue to mount.

Even with the additional steps taken by the US government (USG), it will continue to be difficult to stem the rising tide of cyber-attacks and cyber-espionage. It can be compared to plugging holes in a boat riddled with small holes and more holes appearing all the time. Some have advocated the rapid employment of artificial intelligence, advanced machine learning, and other high-technology tools to augment the professionals battling myriad current threats, but those solutions may be years or more away. The need for more cyber-defense capacity has never been more acute.

The answers to achieve a higher capacity are generally not quick wins, as evidenced by the push for rapid fielding of new technological solutions. The remedies, however, can be lasting and must be multi-dimensional. The concepts of using machine learning and artificial intelligence, teamed with human analysts, are maturing but that technological advance will not solve the entire capacity problem. Initial attempts to increase capacity by utilizing the military services have included a more traditional approach, using the total force. The Air Force not only has reserve cyber units to augment its active-duty cyber warriors, but has also fielded cyber units in the Air National Guard. In addition to reinforcing active-duty efforts, the Texas National Guard activated cyber units to assist school districts and local municipalities affected by ransomware attacks.<sup>[2]</sup>

Current efforts involve officials creating additional capacity in the face of a growing threat. Congressman Tony Gonzales (R-TX), a former Navy cryptologist, is sponsoring legislation to create a National Digital Reserve Corps. The organization would comprise “a group of civilian individuals with relevant skills and credentials to address digital and cyber needs across the federal government.”<sup>[3]</sup> It would fall under the General Service Administration (GSA) and rely on the GSA to allocate additional resources to agencies in need.

The most audacious plans, however, would provide both a relatively short-term increase in manpower and a long-term, possibly multi-generational, approach to building a cyber-smart military, workforce, and citizenry. Some lessons from current organizations provide possible paths to that bold objective.

### *Using Lessons from History*

In the past, the US has been able to successfully react to rising threats in relatively new domains of warfare. Studying analogous situations and environments and drawing implications for cyberspace provide apt analogies that can help investigate possible strategies for cyber-related approaches.<sup>[4]</sup> Two organizations provide examples of how we can proceed in adding capacity and improving the nation’s cyber readiness.

By the First World War, the air domain had demonstrated its potential and the US was devising ways to gain advantage. Although the air domain could arguably include balloon observations in the Civil War, the direct destructive power of the airplane had manifested in the First World War and made clear to all that airpower would have a significant role in the future of warfare.

There were several organizations and initiatives aimed at improving the military capability of the US in this new domain. Many of these organizations found it was also important to generate civilian enthusiasm in this area for commercial and research purposes. One such organization was the Civil Air Patrol (CAP), founded by a World War I aviator, Gill Robb Wilson.<sup>[5]</sup> He returned to the United States from Germany in 1936 convinced that a war was brewing in Europe and realized the US needed additional aviation capability, capacity, and education. The CAP was official established by the Commerce, Navy, and War Departments in late 1941 after Wilson's organization consolidated several other flying organizations into a larger, more organized group. Before and during World War II, the group flew anti-submarine patrols off the Atlantic and Gulf coasts. In 1942, the group added a Cadet program that educated teenagers in aviation. Following the war, the CAP was placed under the newly created Department of the Air Force as the branch's civilian auxiliary.

In addition to augmenting patrols on the West coast of the US during World War II, CAP worked with local civil defense programs in planning and execution drills. Later, CAP began to assist local authorities in search and rescue operations. As crash locator beacons became more prevalent in civil aviation, the Air Force directed CAP to begin assisting in search and rescue operations responding to possible incidents with small civil aircraft. Today, the CAP also assists in mass casualty and disaster relief operations/exercises around the country. Thus, CAP provides invaluable additional capacity and sometimes free up assets to work in other areas.

Beyond its operational missions, CAP runs a robust cadet program that includes several benefits. First, it teaches cadets ages 12-21 leadership through a testing regimen and participation in exercises, search and rescue missions, and other programming. More importantly, however, cadets learn about all aspects of aviation. Educational materials provide a thorough history of aviation, from the Wright Brothers to some of the most recent developments in the aerospace industry. CAP has programs to teach cadets to fly with both ground school and flying instruction. The programs instill a lifelong interest in aviation and help propel many to careers in the aviation industry.

The U.S. Coast Guard Auxiliary (CGAUX) is another organization that can be an example for a future cyber auxiliary. The CGAUX was created in 1939 and for over eighty years has assisted the Coast Guard with patrolling, search and rescue, and educational programs. It provided 50,000 members at the beginning of World War II to assist in patrols, and over time, increased capacity by placing many private vessels into service.<sup>[6]</sup>

Today the CGAUX is visible on US waterways and is well known for its boater education and outreach. To promote and improve safety, the CGAUX provides instruction at all levels, thereby improving proficiency, and instilling a love for boating. Courses include operations, maintenance, navigation, and safety topics as well as what to do in an emergency. The CGAUX also plays an important role in providing additional capacity for the Coast Guard during disaster relief, search and rescue, and pollution response. The additional capacity provided by the CGAUX has saved many lives and allowed the Coast Guard to focus on core missions and situations that demand its more specialized equipment and training.

### *A New Approach*

What then, can cyber policy experts gain from familiarizing themselves with CGAUX and CAP? Both organizations offer insight into how cyber leaders can organize, train, and develop capacity in citizens thus providing additional capacity in times of crisis. First, a United States Cyber Auxiliary could embrace education as a core mission. There are several groups that provide cyber education and training, but none resemble an organization like the CGAUX, which is respected, well known, and offers a lifelong education. A cyber auxiliary could provide classes around the country at little or no cost. The audiences would be varied, from novice users to system administrators from those undergoing elementary education to senior citizens. Classes would likely have to concentrate on the defensive side of cyber activity, including basic concepts of information security, password strength/protection, and how to identify suspect emails and websites.

Education options would include a mixture of online and in-person courses and could also bridge the gap between the general population and organizations like the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA). A cyber auxiliary could help those organizations push critical messaging to the public and educate them regarding available resources. Another education-related role would include the advertisement of cyber-related grants and scholarships, coordination of educational efforts in cyber education, and incentivizing cyber careers through scholarships and grants.

The second approach a cyber auxiliary should consider is the inclusion of a cadet program. The shape and feel of such a program would ultimately be dependent on the parent organization of the auxiliary, but a cadet program would accomplish several goals that cyber experts have advocated for many years. First, a cadet program is another way to deliver cyber education, albeit the program would likely be much more rigorous than what would be offered to the general population through the auxiliary. Next, a cadet program builds leadership skills and develops youth who may be interested in government, military, and/or adult auxiliary service in the future. Finally, the program would inculcate an appreciation of cyber skills and instill a desire for lifelong learning in the cyber environment.

Another reason to create a cyber auxiliary would be to build greater capacity for USG cyber organizations. This aspect of the auxiliary might raise concerns, but a few key items can make it focused and effective. The auxiliary would have to be granted authorities to operate but would likely be limited to defensive cyber operations. Much like the educational curricula, any auxiliary cyber operations will be limited to augmenting defensive cyber protection and recovery. The auxiliary could, like the CGAUX, perform regular patrols and assist local government and businesses with network assessments in conjunction with the educational mission. Alternatively, a cyber auxiliary could be activated by a USG parent organization during times of crisis to work on a portion of cyber response or work along USG cyber operators to build capacity, although still limited to defensive cyber operations.

A cyber auxiliary could deliver education and house a cadet program under several elements within the USG. For an organization to assist in active cyber defense operations, it would have to be associated with a department with an active cyber mission and existing authorities. The sponsoring organization would have to exercise tight control over the adult auxiliary volunteers through training, exercises, and emergency procedural powers. Although, the CAP and CGAUX are associated with the Air Force and the Coast Guard respectively, there is nothing preventing a cyber auxiliary from being associated with USCYBERCOM, under the Department of Defense (DoD). A possible alternative could be DHS, which has a much closer tie to civil defense and local protection and mitigation needs. A third option could involve both DoD and DHS, activating auxiliary members to support DoD in case of a national emergency.

No matter what organization a cyber auxiliary eventually falls under, the controls on using auxiliary cyber personnel online must be stringent. The Army has exercised pairings between the active and reserve/national guard components for training and readiness. Cyber auxiliary members could sit alongside USG personnel (military or civilian) during training and exercises, ready to return for operations if the need arises. This portion of the auxiliary would likely take the longest to realize, but could be transformational. Any organizational approach, however, would need to retain an education aspect and possible cadet program to realize the long-term, multi-generational benefits such programs could ultimately achieve.

## **CONCLUSION**

Cybersecurity is now viewed as an important ingredient to myriad functions of society, from the public sector to private industry. The opportunity technology presents must be protected by strong security from a growing number of threats, both state-sponsored and non-state actors. As the threat grows, so too must the effort to protect vital technological resources.

As detailed in this article, a cyber auxiliary can provide both a near-term and long-term solutions to a dynamic threat landscape, which will continue to grow and evolve. There are, however, actual costs involved and significant bureaucratic hurdles to overcome to implement such a multifaceted solution. The expense of establishing any organization can be daunting, especially in an environment that has growing regulatory requirements. There are ways to structure an auxiliary that could limit initial costs and continuing operational expenses. A Public-Private partnership has been a favorite approach of late to cybersecurity and could help jump-start an auxiliary. Another option, similar to CAP or CGAUX, you can tie the organization to an existing agency or service.

In analyzing the options for structures to address concerns with costs or oversight, bureaucratic impediments and resistance to new models will need to be addressed. Unlike CAP or CGAUX, there is no service to attach a cyber auxiliary to, but several organizations have possibilities. To explore options like the U.S. Digital Service, USCYBERCOM, or GSA, new forms of oversight and operational control will have to be developed, tested, and trusted to make a cyber auxiliary work. Legislators and administrators must about the present and the shape of things to come to ensure a capable and nimble organization is formed that can provide the additional capacity the nation requires.

Although the costs of creating a cyber auxiliary can be viewed as an uphill battle, the benefits of an organization that can bring capacity, education, workforce development, and awareness would be truly revolutionary. Recent events have demonstrated the need for the ability for everyone to understand the threat and the necessity of additional cybersecurity capacity during a crisis. The nation will not have the luxury of debating how to increase its capacity to defend against cyber adversaries much longer. The time to find solutions is now.🛡️

## NOTES

1. William T. Eliason, "An Interview with Paul M. Nakasone," *Joint Force Quarterly* no. 9, 2 (2019).
2. "'Holy moly!': Inside Texas' fight against a ransomware hack," KALB, accessed January 15, 2022, <https://www.kalb.com/2021/07/26/holy-moly-inside-texas-fight-against-ransomware-hack>.
3. "Representatives Tony Gonzales, Robin Kelly Introduce Bill to Form National Digital Reserve Corps," press release from July 29, 2021, accessed on January 15, 2022, <https://gonzales.house.gov/media/press-releases/representatives-tony-gonzales-robin-kelly-introduce-bill-form-national-digital>.
4. Robert Axelrod, "A Repertory of Cyber Analogies," in *Cyber Analogies* (Monterey: DoD Press, 2000), 108-116.
5. "History of Civil Air Patrol," Civil Air Patrol, accessed August 25, 2020, <https://www.gocivilairpatrol.com/about/history-of-civil-air-patrol>.
6. "About the Auxiliary," United States Coast Guard Auxiliary, accessed August 25, 2020, <http://cgaux.org/about.php>.

JEFFREY FAIR



# AI, Super Intelligence, and the Fear of Machines In Control

---

Brian Mullins

## INTRODUCTION

**T**he advent of Big Data is decades old, and the citadels built atop its resources have redefined the landscape, shifting the power balance away from governments and into the gray area between the public and private sectors. Regulatory systems have yet to keep pace. Power has come not so much from the collection, ownership, or acquisition of data, but more from the ability to direct them into strategic assets. The combinations of what you know and who knows what will become the next decade's most valuable commodities, with those resting on fractured and ineffective decision-making systems losing the competitive battle.

However, it's important to avoid the superstition of superintelligence, waiting for - or fearing - the day that the machines awaken and take control. The ultimate battle will not be between humans and machines. The battle will be hybrid means and those harnessing the power of true human-machine collaboration will come out on top, thereby achieving true organizational intelligence. This article addresses the foundations of organizational intelligence, and how to navigate the shifting sands and strengthen one's financial and reputational position within global power dynamics.

## WHAT DO WE KNOW?

The volume of currently accessible data is unprecedented. The World Economic Forum estimates this will reach 44 zettabytes in 2020.<sup>[1]</sup> By 2025, data generated globally each day is projected to reach 463 exabytes, or 175 zettabytes in total,<sup>[2]</sup> and by 2025 there are likely to be 30 billion Internet of Things (IoT) device connections worldwide, equating to nearly four for each person on the planet.<sup>[3]</sup>

© 2022 Brian Mullins



**Brian Mullins** is a graduate of the U.S. Merchant Marine Academy. He is an entrepreneur and technical leader with over a decade of experience in high growth technology companies as CEO, scaling teams from just a few, to hundreds of employees across 4 countries and raising over \$330 MM in investment capital. Serving on the frontiers of technology, he has been awarded over 100 U.S. patents, has testified as an expert before the U.S. Senate, received an Edison award for Industrial Design, been named a CNBC Disruptor 50, and was one of Goldman Sachs “100 Most Intriguing Entrepreneurs.”

In 2019, Brian joined Mind Foundry, an Oxford University company as CEO. Mind Foundry specializes in high stakes applications of AI across the sectors of Insurance, Government, Security and Defense.

This trend continues to grow extraordinarily and there is no denying that our obsession with data capture in the quest for insight has changed entire industries. To clarify, data itself is not information. Moreover, information is not intelligence. More data does not translate directly into better decisions, and this is the first myth of control.

***The first myth of control: more data equals more knowledge***

Historically, lack of information has driven uncertainty. We have moved from a world replete with ignorance, to a world saturated with information but still lacking in evidentiary support for decision-making. We are now blessed with an excess of data, but the quest to capture as much information as possible has now found itself at the feet of intelligence. Navigating this dense data landscape has provided us with architectures, technologies and even entire industries dedicated to the pursuit of insight and intelligence. Assessing what you know, and with what certainty have become key beacons of the information age.

Artificial intelligence itself has risen in prominence with the ever-increasing ability to crunch and then translate large amounts of raw data into information-rich assets. While data is created, analyzed, and sometimes tortured to extract its perceived full potential, machines are deployed to sift through mountains of available data to refine more valuable assets. Data as a commodity has been compared to oil.<sup>[4]</sup> The more data you own, control, and use, the more power you have. Instead of sitting on top of an oil well, you are sitting on top of an infinite well of data at one’s disposal. But the analogy stops here. Oil is finite, yet data is - for all intents and purposes - infinite. Oil is single-use, while data can be created and re-used, and exist in many different forms. You are sitting on, and continuously collecting, an asset whose potential, given the right conditions, can increase in size and value over time.

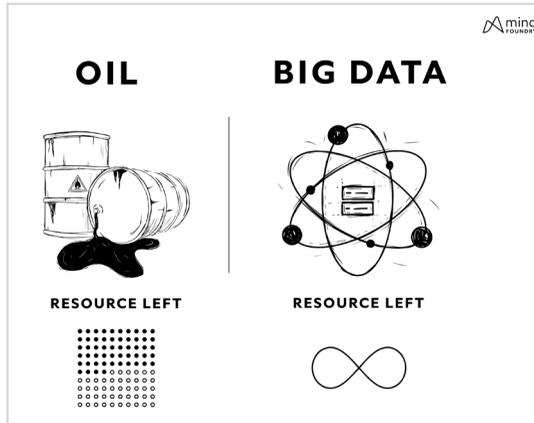


Figure 1. Oil and Big Data Resources. Mind Foundry 2021.

One’s ability to process, refine, curate and sustain assets helps define success in this new age. Maintaining evidentiary chains of custody for these assets and capturing their use in decision-making are foundational tools needed by all. This in turn has led us from ignorance being understood as ‘not knowing’, to now being defined as ‘not knowing enough.’

***The Myth of Superintelligence***

In the pursuit of knowledge, we’ve fallen prey to various theories of superintelligence. A common thread among these theories is that more data coupled with ever more powerful machines will produce superintelligent machines. The idea that a machine or series of machines will suddenly be endowed with sufficient data or computational power to qualify as ‘superintelligent’ is worse than unrealistic – it is superstitious.

The commoditization, fragmentation, and complexity of the data landscape alluded to above requires increasingly more sophistication to manage. There is reason to believe that Moore’s law – the observation that computational capacity doubles roughly every two years as the size of transistors gets smaller – is becoming more inaccurate.<sup>[5],[6]</sup> What happens when the amount of computation power plateaus, dependent not solely on power, but also mineral resources for chips?<sup>[7]</sup>

Worse, we still quake so much in the shadow of impending technological singularity that we foist misdirected control systems on semi-autonomous systems in the hope of keeping them in line and buying ourselves time to stop an ‘intelligence explosion.’ Our focus should be on how we can rise above this fear and build a world where we can interoperate with trust.

***The second myth of control: a human will always have the final say***

We need to more fully understand what governance and oversight look like in this space. Outdated methods, including human-in-the-loop, are increasingly becoming inadequate fail-safes. In the face of automation, these human-speed inefficiencies will become primary automation targets, taking with them incumbent security mechanisms. In a truly hybrid domain, the

efficiencies of human and machine agents operating on collaborative tasks require more sophisticated mechanisms of oversight. The best path towards a governance framework that will optimally fit an AI-enabled workforce begins with a basic understanding of the hybrid systems – everything from their benefits and known failure modes to their interactions with each other.

## **SO, WHO KNOWS WHAT?**

We have been too obsessed with the pursuit of data-driven knowledge – so much so that subsequent action is sometimes an afterthought. The true performance indicators of how well an organization is harnessing its incumbent knowledge are often poorly architected or understood.

The intelligence-processing domain provides a good example. As in many industries, the tsunami of data at the intelligence community's disposal exceeds human processing capability. There are established methods for data collection and connection, for disseminating intelligence reports, and for creating actionable products. There is an entire domain dedicated to the processing of intelligence data, which involves multiple layers of sanitization. This is no mean feat but generally, the field-to-field delay time is too long.

A piece of information collected yesterday that is not actionable until tomorrow – or three months from now – represents an intelligence chain that at best is sub-optimal, and at worst, broken, and undermines the effectiveness of those whose job depends on decisions and action that can exploit that information. Given the stakes, many industries simply can't afford such delays. Even where incumbent capabilities exist, efficiencies break down when the systems cannot achieve the necessary performance. From an organizational perspective, this can be the ability to act as desired within a particular time frame, or simply to act in general.

### ***The third myth of control: once something is known, everyone knows it***

That someone somewhere knows something is insufficient. Living in a connected world, we assume that once something is known that it is immediately disseminated to everyone that needs to know it, which simply is not the case, even within tightly knit organizations. Mechanisms to enable effective organizational decision-making require explicit architecture and thought. Also required is the ability to adapt rapidly as the environments around us change. Relying solely on broadcast mechanisms simply amounts to turning up the volume and letting the noise get louder. It is better and smarter to build systems that effectively get the right information to the right person at the right time.

## **WHERE WE GO FROM HERE**

Whilst writing this article, I was lucky enough to get the thoughts of Professor Stephen Roberts, Director of the Oxford University Center for Doctoral Training in Autonomous Intelligent Machines and Systems. Our conversation touched upon how we must begin from a systemic vantage point to design systems that interface with the complexity of data and a range of

human and machine stakeholders. He commented that, “we live in an era of hyper-abundant data. However, solving the challenges we face requires more than data alone. It requires a deep understanding of the dynamic relationships found not only in the data, but also between agents and stakeholders associated with it; as generators, consumers or actors within the data-sphere. Understanding such complexity hinges upon our abilities to create robust models able not just of dissecting complex data, but capable of managing and orchestrating its flow and engagement across stakeholders, be they software, hardware or human agents.” (Professor Stephen Roberts, Personal Interview, December 2021). Thus, not only must we be able to harness and operate on the increasingly vast amounts of available data; we also need to anticipate and direct our data-collecting activities towards those most valuable. Finally, we need a way to imbue our values and principles into the systems we design and use, and to better understand what true human-machine collaboration looks like, with reliable performance indicators that will ensure immediate and long-term success.

This is not so much about learning how to harness AI as a tameable beast, but more about how to bring it into your team as a trusted and responsible member. This is best achieved by ensuring an unwavering commitment to continuous organizational learning that enables both human and synthetic agents to learn and improve as they collaborate towards defined goals.

This was touched upon further when I recently connected with Professor Mike Osborne, one of the world’s leading experts in collaborative AI technologies, from Oxford University’s Machine Learning Research Group, we discussed the necessity to embed human context in the design of artificial intelligence systems. Mike explained that, “It is misleading to think of AI today as being a like-for-like replacement for a human worker. AI today is powerful, but severely limited. Even with today’s data volumes, AI without deep human collaboration is useless at best and harmful at worst. The best data that exists is embedded in the heads of those stakeholders who best understand the problems to be solved – only if an organization designs its AI solutions with and around those stakeholders will it truly deliver value.” (Mike Osborne, Personal Interview, December 2021).



Figure 2. Organizational Intelligence. Mind Foundry 2021.

## WHERE DO WE SEE THIS OPERATING AT SCALE TODAY?

Organizational intelligence is not superintelligence as defined by philosopher Nick Bostrom<sup>[9]</sup> and others. Today, the hallmarks of superintelligence are seen not in our machines, but rather, in the organizational effectiveness of some governments and major corporations. This requires a large orchestration of humans and technologies, the dissemination of information, and decision-making against common goals. This interconnected network of agents working together is the seed from which true organizational intelligence will sprout.

Taking a subset of these organizations – those with the desire and the commitment to harness the true potential of the data age – and providing them with the tools to collaborate with their AI counterparts, you will see a new kind of superintelligence evolving a truly scalable hybrid intelligence.

## BARRIERS TO ORGANIZATIONAL INTELLIGENCE

Organizational intelligence is difficult to achieve, and goes well beyond simply adding AI capabilities to your toolbox or hiring lots of good data analysts and hoping for the best. Of the many impediments to the true realization of organizational intelligence, these are the top four killers:

### *Rigidity of organizational structures*

For centuries certain outfits have enforced control by relying on archaic and rigid chain-of-command structures. While clarity in autonomy for decision-making has its benefits, examples where rigid, inflexible structures are unsuitable abound.

Retired U.S. Navy Captain and best-selling author, L. David Marquet, sees bringing decision making closer to key information as pivotally important, enabling a distributed (or federated) decision-making environment that allows for fast, informed decisions untethered, or at least less tethered, to a central chain of command. Immediate access to relevant and evidenced intelligence should enable strong, even prescient, decisions, provided the organization can make decisions as quickly as that information is made available.

There will always be decisions that cannot and should not be outsourced, and any organizational intelligence framework must be vigilant regarding autonomy given to agents, both human and AI. Humans can adapt well to broad context and new situations. Hybrid organizations must harness this adaptability.

### *Innovation in high-stakes environments*

There is always a complex interplay between evidence-based innovation and the new evidence that arises from that innovation, and as stakes increase, so too do barriers. To test novel technology and can afford a million failures before performance attains success, fine.

One can afford to lose a million chess games, but it is obviously unacceptable when human lives are on the line. I simply note here in passing those valid fears often dampen innovation in high-stakes environments, which often results in the continued use of archaic strategies.

*Failure to adapt*

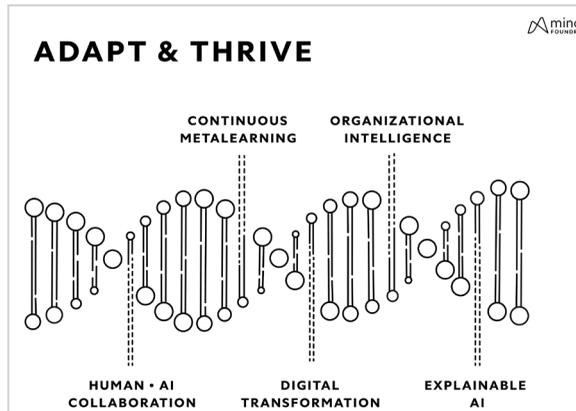


Figure 3. Adapt & Thrive. Mind Foundry 2021.

Current industry standards are insufficient to tackle the demands of the big data age head-on. Solutions designed to mitigate today’s issues, standing alone, will not help us surmount future hurdles. With change as the one constant we all must live with, adaptation must always be the cornerstone for any successful organizational strategy. Data also is in a constant state of flux, as are our technological capabilities. Thus, our response must be continually dynamic.

Even the most mature AI technologies shouldn’t lull us to assume that the future will resemble the past, which includes the data we now collect and hold. Ability to handle a future that looks nothing like the past grows ever more important. While one approach might be to stay at the cutting edge of new technologies, this is only a partial solution. Nimble adaptability is needed at the organizational and human level to optimize the modern-day hybrid workforce. Again, change is our only constant, so while investment in the future is crucial, adaptation needs to be part of a business’s everyday operations.

**THE QUESTION IS ONE OF TRUST**

Each pitfall flagged above can kill organizational intelligence in its crib. So, how is this problem averted?

Trust and accountability are central to a hybrid workforce: they enable autonomous and semi-autonomous AI agents to execute their remits effectively with proper collaborative and auditable functions. Accordingly, both the human and AI agents must:

- ◆ understand their remits and their allowed space of operation,
- ◆ definitively explain their reasoning for making certain decisions,
- ◆ indelibly explain any actions they have taken based on those decisions, and
- ◆ collaborate effectively with other agents against combined problems.

## **THE NEW AGE**

These tenets comprise the backbone of trust and accountability. Increasing amounts of autonomy should not be granted to systems that fall short of these imperatives. This is a pivotal moment: our next steps will reshape the workforce. The sheer amount of available data will continue to expand geometrically. Those who prioritize quantity and the status quo over quality, understanding, and adaptation will lose out. The new age will not find machines ruling us, or humans working within archaic organizational structures. The new age should (and will, if we do this right) find humans and machines working complementary, with the lag between data and action significantly reduced, and human-AI collaboration much better serving the interests of mankind.🛡️

## **NOTES**

1. How much data is generated each day? WEF, April 2019. (1 zettabyte = one trillion gigabytes)  
(1 exabyte = one billion gigabytes)
2. The Digitisation of the World IDC, November 2018.
3. IoT Statistics, Finances Online, 2020.
4. The world's most valuable resource is no longer oil, but data, *The Economist*, May 2017.
5. We're not prepared for the end of Moore's Law, *MIT Technology Review*, February 2020.
6. Compute trends across three eras of Machine Learning, 2022.
7. Kate Crawford, Atlas of AI, 2021.
8. Expanding AI's impact with organizational learning, *MIT Sloan Management Review*, October 2020.
9. Nick Bostrom, How long before superintelligence? updated 2008.



# THE CYBER DEFENSE REVIEW

◆ RESEARCH ARTICLES ◆



# Information as Power: Evolving US Military Information Operations

*and their  
Implications for  
Global Internet  
Governance*

Dr. Milton Mueller

Dr. Karl Grindal

## INTRODUCTION

The 2016 Presidential election that brought Donald Trump to the White House was a turning point in US policies and attitudes toward Internet governance. The discovery of organized Russian influence operations combined with the unexpected election result, led to a fundamental reappraisal of the security implications of the content flowing over global social media.<sup>[1]</sup> Once seen as a realm of civil society subject to communications or technology policy, social media exchanges are now perceived by many as an arena of geopolitical conflict. The US, many claimed, was engaged in information warfare in a way that implicated national security.<sup>[2]</sup> This article explores the consequences of the changing perception of Internet content for US military doctrine regarding Information Operations (IO) and the US approach to Internet governance. The article seeks to answer the following two research questions (RQ):

**RQ1:** What changes in US military organization, policy, doctrine, and practice regarding IO took place after 2016?

**RQ2:** Are the post-2016 US military organizational structures, doctrines, policies, and practices eroding the distinction between liberal-democratic and authoritarian political systems regarding free expression on the Internet?

The motivation for these two research questions is the potential clash between the free expression principles underpinning liberal democracy and concepts of information warfare or state-sponsored influence operations. Constitutional protections constrain governments from censoring and propagandizing their citizens in liberal democratic states. The freedom and autonomy of public expression are perceived to be essential components of democratic self-governance, and state-backed influence operations would undermine them.



**Dr. Milton Mueller** is a Professor at the Georgia Institute of Technology (Atlanta, GA, USA) in the School of Public Policy and Director of Georgia Tech's Master of Science program in Cybersecurity Policy. His most recent book is *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace* (Polity, 2017).

The long controversy over the Smith-Mundt Act of 1948 exemplifies these tensions. The law was passed during the early stages of the Cold War and it authorized US civilian agencies to engage in public diplomacy as part of the ideological competition with the Soviet Union. The law's passage was followed by six decades of controversy over whether the U.S. Information Agency (USIA) produced government propaganda and whether the government could legally disseminate its products to Americans.<sup>[3]</sup> While these concerns pertained to civilian agencies, similar suspicions about Department of Defense (DoD) support for domestic propaganda efforts repeatedly surfaced during the wars in Iraq and Afghanistan.<sup>[4]</sup>

Authoritarian states, in contrast, suffer from no such competing tensions; they openly engage in institutionalized IO against their own citizens. Moreover, their domestic censorship and propaganda activities are justified on national security grounds. Liberal democracies tolerate the instability generated by competing media outlets, political parties, and belief systems, seeing them not only as individual rights but as beneficial to accountability and effective self-governance. In contrast, authoritarian countries make the exchange of ideas and information part of the political and security interests of the state. It follows that there must be fundamental differences between the way authoritarian states and liberal democracies handle the relationship between government IO and national security. Therefore, any significant shifts in the scope or nature of military IO by a liberal-democratic power raise important policy questions.

## METHODOLOGY

The researchers address RQ1 by systematically reviewing DoD memoranda and publications related to IO. This evidence enables differentiation between military doctrine, public policy, and organizations associated with IO before and after 2016. The analysis begins



**Dr. Karl Grindal** is a Postdoctoral Fellow and Instructor at the Georgia Institute of Technology's School of Cybersecurity and Privacy. He received his Ph.D. from Georgia Tech's School of Public Policy in 2021.

with the U.S. Special Operations Command's (USSOCOM) formation in 1987 and ends with documents published in the first half of 2020. The review included documents produced by DoD and the Joint Chiefs of Staff, publications by the different service branches (Army, Navy, Air Force, and Marines), interviews with practitioners, and journalistic sources. The review also included relevant Congressional legislation, reports, hearings, and general literature and case studies on IO published by academic scholars and military theorists. Because the article focuses exclusively on the military response, it did not review the evolution or documentation of civilian agency practices and policies.

The second research question (RQ2) builds on the answers to RQ1 to conduct a qualitative analysis of how evolution in policy, doctrine, and organization exhibits a change in the US approach to global freedom of expression on the Internet. The researchers identify the rationales for the changes and compare them to the justifications offered by authoritarian states. There is also an assessment of the consistency of the new policies with prior US positions regarding Internet governance and Internet freedom.

## WHAT IS IO? DEFINITIONAL ISSUES

Information and information technology have always played a critical role in warfare. Command and control of weapons and troops, intelligence gathering, and counterespionage are central to military operations.<sup>[5]</sup> The US military uses many different labels to describe activities associated with information and cyberspace. In addition to IO, the terms used include information warfare (IW), influence operations (another IO), psychological operations (PSYOPS), propaganda, public affairs, civil-military affairs (CMA), political warfare, active measures, and disinformation.<sup>[6]</sup> These US military concepts and practices cover an expansive, complex, and constantly evolving arena of thought and action.

For simplicity of exposition, this paper will use the label “IO” as an umbrella term for all the aforementioned labels (IW, IO, PSYOPS, CMA, active measures, disinformation). Our analysis, however, will attend to the essential differences in the definitions and connotations of each term, when necessary. The definition of Information Operations given in Joint Publication (JP) 3-13 (2012) is typical and very similar to the definitions of PSYOPS, Military Information Support Operations (MISO):

Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups and individuals. Its target audience includes not just potential and actual adversaries, but also friendly and neutral populations.<sup>[9]</sup>

Adding to the complexity, military concepts related to IO have often been lumped together with military approaches to *cybersecurity* and *cyberspace* in potentially confusing ways. Here, too, we find a host of different labels for various specialized functions, such as cyberspace operations (CO), computer network operations (CNO), and electronic warfare (EW). However, there is a critical distinction between what is defined as IO above and these cybersecurity-related functions. CO and CNO defend or attack the confidentiality, integrity, and availability of *information technology systems*, and EW focuses on attacking or protecting the availability of the electromagnetic spectrum. In other words, CO/CNO/EW manipulate *machines* in cyberspace.

On the other hand, IO produces and manipulates messages to influence the cognition, perceptions, or beliefs of *humans*. While IO may use cyber-technical means to distribute messages, the arena of action is the human mind, not the machines per se. In military parlance, they operate in different domains.<sup>[10]</sup> The critical distinction is that cybersecurity-related operations do not, for the most part, avail themselves of symbolic meaning to humans to achieve their effects.

The existence of multiple, nonintegrated concepts and labels makes the analysis of post-2016 changes in doctrine, organization, and practice more complicated but also more interesting and relevant. Do the doctrinal changes combine these heterogeneous concepts and labels into a single construct or combine them under a single military command? Is the target a state actor in foreign countries with whom the US is engaged in hostilities, or is it a broadly defined Information Environment that includes everyone? Does IO happen only in wartime or also in peacetime? We engage with each of these questions while analyzing the changes in IO before and after 2016.

## TIMELINE AND EVOLUTION OF US IO

Our attempt to track the complex, often-confused evolution of IO concepts in the US military begins in 1987, with the formation of USSOCOM. Over time, this command came to operate as an almost distinct service branch, and set the baseline for IO policy, doctrine and operations for over twenty-five years, until the disruption of 2016.

### *The IO situation prior to 2016*

During the Cold War, the USIA was the government's leading instrument of informational power.<sup>[11]</sup> After the fall of the Soviet Union, the budget and programs of USIA were rapidly curtailed. The human domain set of IO capabilities eventually found a post-Cold War refuge in the new Special Operations Forces (SOF). The Secretary of Defense assigned to USSOCOM all Army and Air Force PSYOPS and Civil Affairs (CA) units.<sup>[12]</sup> USSOCOM's second commander, General Carl Stiner, pushed through an initiative designating PSYOPS and Civil Affairs as part of the SOF and command and control of these units in peacetime as well as wartime.<sup>[13]</sup> Concurrently, information operations was added to USSOCOM's principal mission list.

Linking PSYOPS, CA, and IO with special operations sustained these capabilities and kept them stovepiped away from the other commands. The concentration of IO capabilities in SOF was reinforced by the 9/11 terrorist attacks on the US. The Global War on Terrorism (GWOT) was an arena in which the US faced issues regarding the country's reputation, conflicting ideologies, and psychological influence. Yet efforts to centralize IO capability to support GWOT repeatedly broke down. The Joint Chiefs of Staff established an Information Operations Task Force (IOTF) in the autumn of 2001 as an interagency group to direct information and influence operations and act as the single point of contact for the US government. Nevertheless, according to one military observer, "no other agencies or departments would participate," and its alerts and activities were largely ignored.<sup>[14]</sup> The IOTF was disbanded in July 2002. Special Operations filled the vacuum, becoming "the cornerstone of the US military response to terrorism."<sup>[15]</sup>

Although advocates for integrated IO capabilities in the military criticize the siloing of IO capabilities in SOF, its base in USSOCOM mitigated the policy dilemmas associated with military involvement in propaganda and psychological operations. As one military historian said, it kept them in "a narrow organizational area focused on military and warfighting."<sup>[16]</sup> It also imposed natural limits on the geographic scope of the activity. As two SOF practitioners noted in a 2015 report, the pre-2016 influence operations mindset was suited to smaller-footprint, persistent-presence operations such as counterinsurgency in occupied foreign countries.<sup>[17]</sup> This focus meant that the targets of IO were not engaging with US citizens, and the goals were more narrowly defined and immediate (e.g., convincing locals not to join terrorist groups or to supply information about the whereabouts of insurgents).<sup>[18]</sup> IO was not perceived as a part of great power competition.

However, even under these limited circumstances, issues arose. After 2005 there was a shift in the definition of IO from an integrating function focused on disabling an enemy's military decision making to amorphous notions about informing and influencing civilian populations; this loss of focus contributed to the IO community's slip from relevance in the US military.<sup>[19]</sup> As the possible manipulation of information by the government was viewed with increasing suspicion, a December 2011 Secretary of Defense Memorandum rebranded psychological operations as MISO.<sup>[20]</sup>

A parallel thread developed what became U.S. Cyber Command (USCYBERCOM). Throughout the 1990s and 2000s, society's increasing reliance on computers and the Internet produced within the Intelligence Community a shift from passive to active signals intelligence (SIGINT). According to General Michael Hayden, the move from passive to active SIGINT involved "commuting to the target and extracting information from it, rather than hoping for a transmission we could intercept."<sup>[21]</sup>

In the early days of this shift, active SIGINT<sup>[22]</sup> went under the label of IW. By the end of 1996, however, the term IW was rejected. DoD formally changed IW to IO with the issuance of a new classified order, DoD S3600.1. An unnamed OSD IO official said in an interview with Wiener (2016) that "[t]he State Department made us change terminology from IW to IO for political reasons."<sup>[23]</sup> The "political reasons" appear to be related to the longstanding barriers between state/military propaganda and the civilian environment, which had become increasingly important with the rise of the Internet. Specifically, "the government did not want the inference to be drawn that we are militarizing cyberspace."<sup>[24]</sup> Here we see the constraints and ideals of liberal democracy and Internet governance directly constraining military labels for their doctrine, if not necessarily their operational practice. On the other hand, National Security Agency (NSA) director Lt. Gen. Kenneth Minihan supposedly welcomed the shift as it obscured NSA activities and allowed him to "build out mission capability for Computer Network Attack (CNA) and Computer Network Exploitation (CNE)."<sup>[25]</sup>

The development of cyber capabilities within the Intelligence Community (IC) led to inter-agency squabbling over which service should own Computer Network Defense. Over the next eleven years, the organizational home of offensive and defensive cyber operations changed hands several times and was ultimately subsumed by USCYBERCOM, created on June 23, 2009. USCYBERCOM continued to grow, activating its Cyber National Mission Force (CNMF) in 2014 and being elevated to a combatant command in 2018.<sup>[26]</sup> While CNA was envisioned as having significant warfighting potential, much of the growing scope of USCYBERCOM activities still seemed to fit within an intelligence framework.

Before the creation of USCYBERCOM, there was significant variation in the conceptual understanding of network and IW across the different military services. USCYBERCOM "had the effect of formalizing the interactions among the military services and partially standardizing the thinking."<sup>[27]</sup> Generally, following the creation of the command, the US conceptually distinguished cybersecurity, which involved CNA, CND, CNE, and Electronic Warfare (EW), from human domain actions such as IW or IO. As USCYBERCOM applied a technical understanding of CNA and CNE to its core conceptual mission, the IO community embedded within USSOCOM saw cyberspace as both a vulnerability and an opportunity to shape the cognitive domain.<sup>[28]</sup>

*Evidence of change since 2016*

Since 2016, the perception of information’s increasing relevance to national security has led to military policy, doctrine, and organizational changes. These changes have attempted to reorient IO toward nation-state conflicts, away from its focus in irregular warfare, special operations, and terrorism.

The 2014 conflict in Ukraine already led a few analysts in the US military to focus on Russian IW, or what they called “hybrid warfare.”<sup>[29]</sup> However, while the belief that Russia was pursuing a new approach to IW was gaining credence among specialists in 2014 and 2015, there were no significant changes in policy or shifts in doctrine in those years. It was the 2016 election outcome with the controversy over Russian involvement that brought widespread public attention to Russian IW (and even some exaggeration of it).<sup>[30]</sup>

Measurable changes in policy, doctrine, and organization began in 2017 (see Figure 1) when Russian IW was perceived or asserted to be directly affecting the US, and the threat analysis was enhanced by partisan conflict within the US.<sup>[31]</sup> While latent pockets of support in the military for a new approach to IO may have existed before the 2016 elections, we will show in the following sections that transformative changes to military policy, doctrine, and organizational structure were, at least in part, instigated by perceptions of Russian manipulation of the US information environment in 2016.

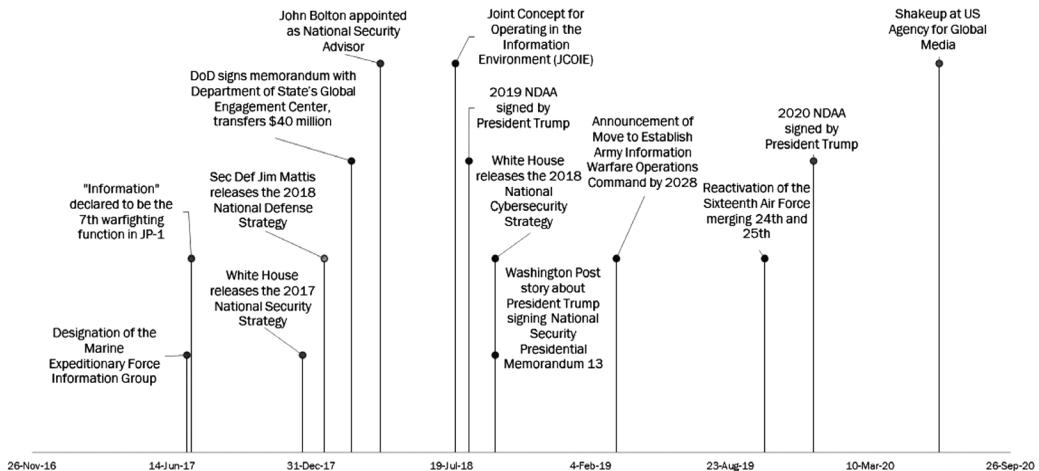


Figure 1. Timeline of Events Related to US Government IO Capabilities.

*Policy*

Strategic national security policy documents produced by the White House, DoD, and Congress identify high-level national security threats and set a corresponding course of action. In the years following the 2016 election interference, these policy documents highlighted the threat of foreign influence operations and sought to empower the US military to counter these threats.

The President must prepare an annual National Security Strategy (NSS), as required by law, that outlines his strategic priorities to Congress.<sup>[32]</sup> Despite President Trump’s downplaying of the role of Russian election interference in 2016, the 2017 NSS contained numerous mentions of the security risks posed by foreign state propaganda and disinformation. This document described how states “weaponize information,”<sup>[33]</sup> and “use cyberattacks for extortion, information warfare, [and] disinformation.”<sup>[34]</sup> Russia is specifically named for “using information tools in an attempt to undermine the legitimacy of democracies.”<sup>[35]</sup> However, both “[s]tate and non-state actors” are identified as “project[ing] influence and advance[ing] their objectives by exploiting information, democratic media freedoms, and international institutions.”<sup>[36]</sup> With the imprimatur of the President, this language authorized the national security apparatus to act against these threats. In contrast, the Obama administration’s 2015 NSS contained only one passing reference to Russian propaganda and never used the terms information warfare, disinformation, subversion, or exploitation of information.

The 2018 National Defense Strategy (NDS)<sup>[37]</sup> altered the US approach to information. It framed information security by describing the actions of US competitors and adversaries as information warfare, political and information subversion, and propaganda. State actions like political and information subversion are identified such that “the homeland is no longer a sanctuary.”<sup>[38]</sup> It further puts this activity in the context of armed conflict, describing adversaries’ use of IW as an example of competition short of open warfare.<sup>[39]</sup>

The President’s 2018 National Cyber Strategy<sup>[40]</sup> further solidified the linkage between information operations and cybersecurity. Unlike the NDS, the National Cyber Strategy is intended to provide guidance across multiple departments and agencies. The 2018 document proposed using all appropriate tools of national power to expose and counter the flood of online malign influence and information campaigns and non-state propaganda and disinformation. It further proposed working with the private sector, academia, and civil society to identify, counter, and prevent the use of digital platforms for malign foreign influence operations.

The Congress’s 2019 and 2020 National Defense Authorization Acts (NDAAs) reaffirmed the national security implications of IO. Section 1642(a) of the 2019 NDAA provided authorities,

[I]f the National Command Authority determines that Russian Federation, People's Republic of China, Democratic People's Republic of Korea, or Islamic Republic of Iran is conducting an active, systematic, and ongoing campaign of attacks [...] including attempting to influence American elections and democratic political processes.<sup>[41]</sup>

The 2020 NDAA under Chapter 19 – Cyber and Information Operations Matters<sup>[42]</sup> reiterates and expands on these authorities with far-reaching language that affirms DoD, “is authorized to conduct military operations, including clandestine operations, in the information environment to defend the United States, allies of the United States, and interests of the United States.”<sup>[43]</sup>

Civilian policy changes, including the NSS, NDS, and NCS, prioritized countering foreign influence operations. Congress then used the 2019 and 2020 NDAs to authorize a significantly expanded role for the military in the information environment. In the subsequent section, we show that the post-2016 agenda setting and expansion of authorities were matched by evolution in military doctrine to address this expanded mission.

### *Doctrine*

Joint Publication 1 (JP-1), the capstone of United States joint doctrine, was amended on July 12, 2017, to incorporate information as the seventh *joint function*.<sup>[44]</sup> As a joint function, information joins intelligence, fires, movement and maneuver, protection, sustainment, and command and control.<sup>[45]</sup> These categories are used to facilitate planning and employment of the joint force.<sup>[46]</sup> Commanders are expected to integrate and balance these functions for effective combat operations. The information function is defined as follows:

The information function encompasses the management and application of information and its deliberate integration with other joint functions to influence relevant-actor perceptions, behavior, action or inaction, and human and automated decision making.<sup>[47]</sup>

Earlier definitions of IO “centered around the notion of attacking enemy communication systems as a way to inhibit the enemy’s exercise of battlefield command and control.”<sup>[48]</sup> With information’s formal designation as the seventh joint function, it is clear that the Joint Chiefs assign to information a much broader concept of IO. Given that both intelligence and command and control were already designated joint functions, the addition of information cannot be understood as relating to battlefield communications or to intelligence gathering. It must mean shaping external information to influence the perceptions and behavior of any relevant actor.

As for how information might be managed, this function is later described as giving joint force commanders “the ability to integrate the generation and preservation of friendly information.”<sup>[49]</sup> While friendly information is not defined, JP-1 notably excluded comments about how the US military will respond/react to unfriendly information. The 2013 edition of JP-1 described how the information environment “includes cyberspace” and thereby defined the cyber domain as overlapping with the information environment.

The Joint Concept for Operating in the Information Environment (JCOIE),<sup>[50]</sup> published July 25, 2018, is a formal expression of the changes in US IO doctrine. As the preface notes, the Chairman of the Joint Chiefs of Staff felt that addressing the role of information in warfare was so critical that he issued an out-of-cycle change to JP-1. The report begins with a 1997 quotation from Richard Jensen which indicates the report’s drafters are already committed to the idea that information war exists and we need to prepare for that eventuality. It implies that the so-called information environment (IE) can create vulnerabilities which can be translated into physical or territorial gains while bypassing the kinetic/physical means of combat. The JCOIE warns that US adversaries are “bolder and accept more risk operating

in this changing IE. As a result, they create political, social, and military advantages that exceed their traditional combat power.”

The JCOIE describes the military challenge of information as one of maintaining “perceptions, attitudes, and other elements that drive desired behaviors.”<sup>[51]</sup> This statement implies that the US military can effectively control perceptions, attitudes, and other psychological factors which drive human behavior. To do this, they need to “integrate physical and informational power ... in an increasingly pervasive and connected IE to produce enduring strategic outcomes.”<sup>[52]</sup>

An acknowledged risk of the doctrine is that “integrating physical and informational power will likely challenge the boundaries of current national policy.”<sup>[53]</sup> These concerns about the boundaries of current national policy expressed in the 2018 JCOIE appear to have been answered in the 2020 NDAA.<sup>[54]</sup>

### *Organizational*

Organizational changes within DoD are moving toward consolidating information capabilities with cyber capabilities. Although there are strong advocates for such consolidation in conceptual terms, this integration faces huge obstacles due to the US military’s complex and divided structure and the overlaps between different informational functions. Inconsistent and contested terminology has left ambiguity over the names of these consolidated entities, particularly as service-level cyber commands merge intelligence and information operations capabilities. The rate of change across the service branches varies, with the Navy having in some way anticipated the trend, the Air Force taking a quick pivot, and the Army establishing a ten-year plan.

The Naval Network Warfare Command (NETWARCOM) brought the Naval Security Group Activities under its command in 2005, incorporating the Naval Information Operations Command (NIOC) into the same organization as the one focused on cybersecurity capabilities. In 2010, this relationship was solidified with the creation of the U.S. Fleet Cyber Command.

The 16<sup>th</sup> Air Force, which was reactivated on October 11, 2019, merged the 24th and 25th Air Forces. The 24th Air Force served as a cyberspace combat force from 2010 to 2019, while the 25th provided intelligence, surveillance, and reconnaissance. While heavily focused on intelligence, the 25th Air Force included the 688th Cyberspace Wing (known as the Information Operations Wing from 2009 to 2013) based at Lackland Air Force Base.<sup>[55]</sup> The 16<sup>th</sup> Air Force is presently known both as Air Force Cyber and as the Information Warfare Numbered Air Force as it merged intelligence, surveillance, reconnaissance, cyber warfare, electronic warfare, and information operations capabilities under a single command.

On March 13, 2019, at AFCEA’s 2019 Army Signal Conference, Lt. Gen. Stephen Fogarty announced his intent to transform Army Cyber Command (ARCYBER) into an Information Warfare Command by 2028. In 2020, IO capabilities were moved to Fort Gordon in Augusta,

Georgia, where ARCYBER was headquartered. At that time, Lt. Gen. Fogarty also reiterated his intentions and his vision for a convergence of capabilities.<sup>[56]</sup> While existing 1<sup>st</sup> IO brigade capabilities are focused on traditional “Operations Security (OPSEC), Military Deception (MILDEC), and IO's core synchronization and integration functions,”<sup>[57]</sup> Lt. Gen. Fogarty targets multidomain capability in 2028 to defeat “adversary Information Warfare by Operations in the Information Environment (OIE).”<sup>[58]</sup> The Army’s conceptual terms continue to evolve, with reports suggesting that “information advantage” has replaced “information warfare” and that the term will soon be incorporated into doctrine.<sup>[59]</sup>

In July 2017, the Marine Corps set up its first information group, the Marine Expeditionary Force Information Group (MIG). Brig. Gen. Roberta Shea described this program as: MIG will provide Marine Corps commanders with the ability to more fully integrate information warfare capabilities into their plans.<sup>[60]</sup> While described as an information group, the officer’s description of MIG capabilities sounded more like traditional cybersecurity capabilities, as they seek to “degrade and detract from our enemy’s ability to access their own networks while also defending our commanders’ ability to maneuver in the information environment.”<sup>[61]</sup>

The previously mentioned 2020 NDAA had a significant organizational component relevant to Information Operations. Section 1631(a) describes the position of a Principal Information Operations Advisor who operates a Cross-functional Team who reports directly to the Secretary of Defense. Changes by the services have been mirrored by calls for an integration of functions under USCYBERCOM. As Lt. Gen. Fogarty stated in July of 2018, “[i]n the future [...] maybe it’s not going to be U.S. Cyber Command; maybe it’s going to be U.S. Information Warfare Operations Command.”<sup>[62]</sup> A December 2020 *Washington Post* article also pointed to this integrated future, as it described how USCYBERCOM is developing IW tactics as a response to the possibility of Russian interference in the 2020 election.<sup>[63]</sup>

## **ANALYSIS AND DISCUSSION OF RQ1**

Two clear changes have taken place in the US military’s approach to information and cybersecurity since 2016. The first is a broadening of the scope of military IO from warfighting in special operations to great power competition in peacetime. This larger scope implies that IO is being elevated from the operational level to the strategic level. The second is a tendency for organizational structures to combine operations in the cyberspace domain with information operations in the human domain.

### ***From Operational to Strategic***

The post-2016 environment has broken IO out of the silo of special operations and irregular warfare. Legislation, policy, and doctrine have shifted explicitly to address ongoing great power competition with China and Russia in the absence of actual military conflict. Congress passed broad authorizations to conduct military operations in the information environment.

Policy has also shifted toward a globalized concept of the relevant Information Environment. These changes exacerbate the policy problems associated with the practice of IO by a liberal democracy. It was easier to maintain boundaries between military IO and the domestic civilian information environment when military IO doctrine was focused on counterinsurgency operations in faraway developing countries. Post-2016, these boundaries are now in tension with globalized social media and great power competition, where the IE is seen as a factor affecting strategic conflict.

### *Greater integration of cyber/IO capabilities*

Russian activities during the 2016 election have mobilized efforts to integrate cyber and IO capabilities. There is strong advocacy within the military to merge and integrate cyberspace-domain capabilities (CO, CNE, and EW) with human domain capabilities such as PSYOPS and IO. The label, Information Warfare, has been suggested as a unifying concept.<sup>[64]</sup> Some advocates of this position hold up FM 100-6 (1996) as a model because it integrated activities in both the human and cyber domains into an organized hierarchy with IO as the umbrella concept.<sup>[65]</sup> Some advocates of this position do not recognize cyberspace operations and IO as operating in different domains. Others grasp the distinction but see cyberspace in a subordinate role as a means for delivering, disrupting, or generating information-related capabilities in the service of broader, human domain objectives. Although rarely stated explicitly, the underlying premise seems to be that control of cyber infrastructure would facilitate the ability to control or manipulate message content in ways that shape attitudes and behavior. While encouraged by the post-2016 policy environment, this tendency has not been victorious as evidenced by Lt. Gen. Fogarty's reversal on establishing an Army IW command.

## **ANALYSIS AND DISCUSSION OF RQ 2: IMPLICATIONS FOR GLOBAL INTERNET GOVERNANCE**

There were three ways in which the post-2016 changes in IO doctrine, policy, and organization affected global Internet governance: (1) there was a tacit acceptance of certain principles regarding information advanced by authoritarian nations; (2) there was a triggering of a security dilemma in the Global Information Environment (GIE); (3) some of the military-civilian boundaries traditionally associated with liberal-democratic governance were blurred.

### *Parallels to the Shanghai Cooperation Organization's 2011 Code of Conduct on Information Security*

One clear manifestation of the Internet governance implications of these changes comes from the de facto, but not widely noted, acceptance by the US of cyber norms promulgated by authoritarian states. The original 2011 draft of the Shanghai Cooperation Organization's (SCO) *Code of Conduct for State Behavior in Information Security*<sup>[66]</sup> included a pledge that each state would do the following:

...cooperate in...curbing the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment.<sup>[67]</sup>

The US, with the support of human rights organizations, interpreted as curbing of information dissemination and as a way of justifying the restriction of international information flows that a sovereign might see as destabilizing or undesirable.

Still, almost every policy and doctrinal move the US has made since 2017 affirms the principles and norms in the SCO's approach to information security. They contain multiple references to political and information subversion. Like China, the US is moving to shut foreigners out of its own National Information Environment (NIE). The Trump administration's proposal to block Chinese apps TikTok and WeChat took this logic to an unprecedented extreme.<sup>[68]</sup> The US has, until recent years, been the world's strongest advocate of Internet freedom and a global, non-sovereignty-based approach to Internet governance.<sup>[69]</sup> For it to back away from those principles is a significant change in global Internet governance.

### *The Security Dilemma in Information*

The security dilemma is an inevitable problem when states in an anarchic system with imperfect knowledge about each other observe and respond to the military activities of their rivals. One state's strengthening can be perceived as aggressive and threatening by another state, increasing the second state's sense of insecurity. This response can lead to a self-reinforcing spiral where both sides generate an arms race.

IO may be creating such a spiral. Ironically, both Russia and the US see IW as something that bad foreigners do, but not something they themselves do. US JP 3-13.2 (2010) defined Propaganda as a form of adversary communication, while in Russian military doctrine Information Warfare is used to describe things done to Russians, not what Russia does to other countries.<sup>[70]</sup> Indeed, the so-called Gerasimov Doctrine that the US military still uses to characterize Russia's approach to IW was not a doctrine at all. Rather, the concept was derived from a talk in which he expressed the view that the Arab Spring and other color revolutions were a form of IW by the US.<sup>[71]</sup> Yet, despite these disclaimers, both Russia and the US use the IW actions of their adversary to justify their own IW initiatives. China could easily fall into the same pattern if it has not already.

Internet-based social media, which already suffers from a deficit of trust, could be further damaged by an IW arms race in which all rival powers engage in competing, military-backed efforts to "to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives."<sup>[72]</sup> A descent into mutual IW by major nation-states could make the depredations of commercially-induced spam and phishing look tame by comparison.

### *Blurring Boundaries*

The new doctrines and organizational structures blur the lines between war and peace, military and civilian activity, and foreign and domestic targets. Although that point is too abstract to be stated explicitly in official military doctrine, some military theorists have already asserted as such. The expansion of warfare from the physical to virtual domains “allows state and non-state actors to bypass military forces to directly reach adversary populations—the human domain—through virtual...means,” and that such “direct access to the human domain in 21<sup>st</sup> century warfare blurs the lines between civilian and military targets.”<sup>[73]</sup> A prominent advocate for having an Information Warfare Command in the US military criticized the “pigeonholing of PSYOPS into a narrow organizational area focused on military and warfighting”<sup>[74]</sup> as “a vulnerability that can be exploited by potential adversaries with pervasive and integrated psychological operations that are also tightly linked to all their public affairs efforts.”<sup>[75]</sup> This implies that operations in the information environment must be perpetual and not confined to specific zones. It is a rather explicit statement that liberal democracies need to mimic the way their adversarial authoritarian states integrate IO functions, which blurs the lines between liberal democracies and authoritarian states.

Cyberspace is so thoroughly connected that a military campaign in the information environment can no longer be targeted at a population easily segmented by nationality or territory. What is the military’s role when there is no distinction between an enemy attack and a marketing campaign by a multinational public relations firm? What is the role of the military when a cultural exchange program is considered a form of IO? If the Geneva Conventions require us to differentiate our treatment of civilians and combatants, how does that happen when one is operating on Facebook’s territory and everyone’s identity is part of an account rather than a country?

Indeed, this expansive concept of war can even blur the line between informational and physical operations. The JCOIE quotes a UK general as saying, “We conduct all operations in order to influence people and events, to bring about change, whether by 155mm artillery shells or hosting visits: these are all influence operations.”<sup>[76]</sup> While it is true that an artillery barrage can be intended to send a signal or shape perceptions, does it also mean that attempts to influence psychology or perception through the exchange of messages are the moral or tactical equivalent of an artillery barrage? If so, such an approach expands our notion of what war is to practically every form of human interaction and in doing so, contributes to the militarization of all information/communications technologies and content. What then happens to the liberal order?

## CONCLUSION

This article surveyed changes in US military organization, policy, doctrine, and practice that resulted from the controversies over Russian influence operations. It then explored the implications of these changes for global Internet governance. Along the way, it cataloged the many different labels applied to the military aspects of information, noting an important distinction between activities targeting the cyberspace domain and those targeting the human domain.

Our findings show that, post-2016, policy has moved IO from the tactical and operational limits of special operations and pushed it up to the strategic level. It is also fostering a merger and integration of US capabilities across the cyberspace and human domains. While the Information Warfare label remains contentious, these integrating trends show up across multiple commands. We found evidence that these changes are at risk of eroding the distinction between the information policies and practices of the US and authoritarian regimes. In addition, broader concepts of strategic IW blur the lines between war and peace, military and civilian responsibilities, foreign and domestic targets. Paradoxically, even as they blur these lines, the concept of IW pushes its adherents to impose national borders on Internet exchanges, a tacit embrace of sovereigntist and nationalist cyber norms that the US explicitly rejected less than a decade prior. 🛡️

NOTES

1. U.S. Senate, Subcommittee on Cybersecurity, April 27, 2017, Hearings on Cyber-enabled Information Operations, <https://www.armed-services.senate.gov/hearings/17-04-27-cyber-enabled-information-operations>. U.S. Senate, 116th Congress, 1st Session. Report of the Select Committee on Intelligence: Russian Active Measures Campaigns and Interference in the 2016 U.S. Election.
2. Kathleen Hall Jamieson, *Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don't, Can't, and Do Know* (New York: Oxford University Press, 2018); "Open Hearing: Social Media Influence in the 2016 U.S. Election," Pub. L., No. 27-398 PDF, § Select Committee on Intelligence (2017).
3. Matthew Armstrong, "A Brief History of the Smith-Mundt Act and Why Changing It Matters," MountainRunner.us (blog), February 23, 2012, [https://mountainrunner.us/2012/02/history\\_of\\_smith-mundt/#.UeBLBD4wY0I](https://mountainrunner.us/2012/02/history_of_smith-mundt/#.UeBLBD4wY0I).
4. Lawrence Sellin, "The Caldwell information ops allegations: It's just military office politics gone wild." *Foreign Policy*, February 28, 2011.
5. Jon Lindsay, *Information Technology and Military Power*, Ithaca, NY: Cornell University Press, 2020).
6. Herbert Lin, "Doctrinal Confusion and Cultural Dysfunction in DoD: Regarding Information Operations, Cyber Operations, and Related Concepts," *The Cyber Defense Review* 5, no. 2 (2020): 89-108, <https://doi.org/10.2307/26923525>; see also the historical list of "Joint Cyberspace Doctrine" definitions in Sarah White, *Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine*, doctoral dissertation, Harvard University, Graduate School of Arts and Sciences, 2019, 12.
7. George F. Kennan, "The Inauguration of Organized Political Warfare [Redacted Version]," April 30, 1948, History and Public Policy Program Digital Archive.
8. Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020). PAGE NUMBER?
9. Joint Publication 3-13. Information Operations (27 November 2012 Incorporating Change 1 20 November 2014).
10. Milton L. Mueller, "Against Sovereignty in Cyberspace," *International Studies Review* 22:4 (2020) 779-801.
11. Donald M. Bishop, "DIME, Not DiME: Time to Align the Instruments of U.S. Informational Power," *The Strategy Bridge*, June 20, 2018, <https://thestrategybridge.org/the-bridge/2018/6/20/dime-not-dime-time-to-align-the-instruments-of-us-informational-power>.
12. USSOCOM, "United States Special Operations Command History: 1987-2007," USSOCOM History (MacDill AFB, FL: USSOCOM/SOCS-HO, 2007), <http://www.fas.org/irp/agency/dod/socom/2007history.pdf>.
13. In 1993, General Stiner's successor (General Wayne Downing) revised the command's mission statement to read: "Prepare SOF to successfully conduct worldwide special operations, civil affairs, and psychological operations in peace and war in support of the regional combatant commanders, American ambassadors and their country teams, and other government agencies" (USSOCOM, 2007, 12).
14. Lt. Col. Susan L. Gough, "The Evolution of Strategic Influence" (Carlisle Barracks, PA: U.S. Army War College, 2003), <https://fas.org/irp/eprint/gough.pdf>.
15. USSOCOM, "United States Special Operations Command History: 1987-2007," 22.
16. Conrad Crane, "The United States Needs an Information Warfare Command: A Historical Examination," *War on the Rocks* (blog), June 14, 2019, <https://warontherocks.com/2019/06/the-united-states-needs-an-information-warfare-command-a-historical-examination/>.
17. Thomas M. Scanzillo and Edward M. Lopacienski, "Influence Operations and the Human Domain," CIWAC Case Studies (Newport, RI: U.S. Naval War College, March 2015), ii <https://digital-commons.usnwc.edu/ciwag-case-studies/13>.
18. Reports in the military focused on operations in the Philippines, Afghanistan, the Sahel, and operations against ISIS.
19. White, *Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine*, 76-77.
20. Secretary of Defense Memorandum, "Changing the Term Psychological Operations (PSYOP) to Military Information Support Operations (MISO)," December 12, 2011, <https://www.marines.mil/News/Messages/Messages-Display/Article/887791/changing-the-term-psychological-operations-to-military-information-support-oper/>.
21. Michael V. Hayden, *Playing to the Edge: American Intelligence in the Age of Terror* (New York: Penguin Press, 2016), Chapter 8. This shift seems to have been advanced by NSA leadership without significant institutional buy-in or congressional direction.

## NOTES

22. Ibid, 134. Active SIGINT is defined by Michael Hayden as “commuting to the target and extracting information from it, rather than hoping for a transmission we could intercept in traditional passive SIGINT.”
23. C. Wiener, “Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as a Major Military Innovation,” Ph.D. dissertation, George Mason University, 2016, 156.
24. Ibid, 156.
25. Ibid, 155.
26. White, *Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine*, 389.
27. Ibid, 24.
28. Joint Publication 3-13 (2014) defines cyberspace as part of the information environment.
29. Timothy Thomas, “Russia’s 21st Century Information War: Working to Undermine and Destabilize Populations,” *Defense Strategic Communications: The Official Journal of the NATO Strategic Communications Center of Excellence*, 1:1 (2015) 10-25.; Mark Galeotti, “The ‘Gerasimov Doctrine,’ and Russian Non-Linear War.” Peter Pomerantsev, “How Putin is reinventing warfare,” *Foreign Policy*, May 5, 2014. Pomerantsev’s original article was widely reproduced, <https://foreignpolicy.com/2014/05/05/how-putin-is-reinventing-warfare/>.
30. Mark Galeotti, “I’m sorry for creating the ‘Gerasimov Doctrine,’” *Foreign Policy*, March 5, 2018. Page number?
31. Office of the Director of National Intelligence, *Russia’s Influence Campaign Targeting the 2016 U.S. Presidential Election* (January 6, 2017).
32. H.R.3622 - 99th Congress (1985-1986): Goldwater-Nichols Department of Defense Reorganization Act of 1986, <https://www.congress.gov/bill/99th-congress/house-bill/3622>.
33. Donald J. Trump, “National Security Strategy of the United States of America” (Executive Office of the President, December 18, 2017), 34.
34. Ibid, 31.
35. Ibid, 14.
36. Ibid, 37.
37. Jim Mattis, “Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military’s Competitive Edge,” (Defense Technical Information Center, January 1, 2018), <https://apps.dtic.mil/sti/citations/AD1045785>.
38. Ibid, 3.
39. Ibid, 3.
40. Donald J. Trump, “National Cyber Strategy of the United States of America” (Executive Office of the President, September 2018), <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.
41. H.R.5515 - 115th Congress (2017-2018): John S. McCain National Defense Authorization Act for Fiscal Year 2019, <https://www.congress.gov/bill/115th-congress/house-bill/5515/>.
42. S.1790 - National Defense Authorization Act for Fiscal Year 2020, 116th Congress (2019-2020). <https://www.congress.gov/bill/116th-congress/senate-bill/1790>
43. H.R.2500 - 116th Congress (2019-2020): National Defense Authorization Act for Fiscal Year 2020, <https://www.congress.gov/bill/116th-congress/house-bill/2500/>.
44. Joint Publication 1, *Doctrine for the Armed Forces of the United States*. 25 March 2013 Incorporating Change 1 12 July 2017 (hereafter, JP-1).
45. JP-1, xii.
46. JP-1, I-18.
47. JP-1, I-19.
48. White, *Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine*, 53.
49. JP-1, I-19.
50. Joint Chiefs of Staff, “Joint Concept for Operating in the Information Environment (JCOIE)” (Washington, DC, July 25, 2018).
51. Ibid, ix.

**NOTES**

52. Ibid, vii-viii.
53. Ibid, 40.
54. H.R.2500 - 116th Congress (2019-2020): National Defense Authorization Act for Fiscal Year 2020. The 2020 NDAA provides a blanket authorization for the Secretary of Defense to “conduct military operations, including clandestine operations, in the information environment” to defend the US and its interests.
55. Lackland AFB also hosts the Joint Information Operations Warfare Center, which coordinates information operations.
56. Stephen G. Fogarty and Bryan N. Sparling, “Enabling the Army in an Era of Information Warfare,” *The Cyber Defense Review* 5, no. 2 (2020): 17-28.
57. Ibid, 22.
58. Ibid, 24.
59. Mark Pomerleau, “U.S. Army emphasizes ‘information advantage’,” C4ISRNet.com, May 5, 2021, <https://www.c4isrnet.com/information-warfare/2021/05/25/us-army-emphasizes-information-advantage/>
60. U.S. Marine Corps Forces Cyberspace Command, “Marine Corps Creates First Information Group to Prepare for Modern Battlefield,” accessed August 11, 2021, <https://www.marforcyber.marines.mil/News/Article/1407775/marine-corps-creates-first-information-group-to-prepare-for-modern-battlefield/>.
61. Ibid.
62. Mark Pomerleau, “Where Do Information Operations Fit in the DoD Cyber Enterprise?” *Fifth Domain*, July 26, 2018, <https://www.fifthdomain.com/c2-comms/2018/07/26/where-do-information-operations-fit-in-the-dod-cyber-enterprise/>.
63. Ellen Nakashima, “U.S. Cybercom Contemplates Information Warfare to Counter Russian Interference in 2020 Election,” *The Washington Post*, December 25, 2019.
64. Fogarty and Sparling, “Enabling the Army in an Era of Information Warfare.”
65. Crane, “The United States Needs an Information Warfare Command: A Historical Examination.”
66. The full text of the SCO proposal can be found here: <https://undocs.org/A/66/359>. The SCO Code was revised and resubmitted to the UN in 2015.
67. Ibid.
68. Donald J. Trump, “Executive Order on Addressing the Threat Posed by TikTok,” Executive Office of the President, August 6, 2009.
69. U.S. support for the administration of the domain name system by the Internet Corporation for Assigned Names and Numbers (ICANN), and the decision to release ICANN from U.S. Commerce Department supervision in 2016 are examples of its commitment to a global governance approach.
70. ОЕННАЯ ДОКТРИНА РОССИЙСКОЙ ФЕДЕРАЦИИ (Military Doctrine of the Russian Federation, 2014), <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=172989&fld=134&dst=1000000001,0&nd=0.29957666907029545#03764223477202755>.
71. *Military-Industrial Courier* (February 2013), <https://www.vpk-news.ru/articles/14632>.
72. This is the definition of “PSYOPS” from JP-1.
73. Lauren Elkins, “The 6th Warfighting Domain,” *Over the Horizon*, November 5, 2019, <https://othjournal.com/2019/11/05/the-6th-warfighting-domain/>.
74. Crane, “The United States Needs an Information Warfare Command: A Historical Examination.”
75. Ibid.
76. Major General Graham Binns, General Officer Commanding, 1st (UK) Armoured Division, cited in the JCOIE (2018), 16.





# “Explicit” Bargains are Essential to Forming Desired Norms in Cyberspace

---

Major Wonny K. Kim

## ABSTRACT

*As the United States endeavors to establish international norms in cyberspace, it is critical to delineate which behavioral norms it supports, how it plans to establish them, and to what ends the norms are to serve. Espionage does not violate any international norm; participants have tacitly agreed to undertake espionage and counterintelligence that fall below the “scale and effects” attributed to the “use of force”<sup>[1]</sup> and assume their associated costs in peacetime. Yet not all espionage in cyberspace below this threshold is considered acceptable. For example, the US desires to bar espionage conducted “with the intent of providing competitive advantages to companies or commercial sectors.”<sup>[2]</sup>*

*Existing literature largely favors tacit bargaining to develop norms in cyberspace. However, the dynamics of the 2015 U.S.-China Cyber Agreement highlight the necessity of both explicit bargains and the prospect of cooperation to avoid costly escalatory spirals. The newly established position of Deputy National Security Advisor for Cyber and Emerging Technology and the formation of Department of State’s Bureau of Cyberspace and Digital Policy offer a chance to develop a US-led multi-lateral whole-of-government approach for the formation of cyberspace norms. This approach is discussed here, using the the U.S.-China Cyber Agreement to illustrate how it would be preferable over simply relying on tacit bargaining.*

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



**Major Wonny K. Kim** is an Innovation and Information Operations Officer in the U.S. Army Reserve 75th Innovation Command and has served at various echelons in Europe, Africa, and the Middle-East. He holds a Master of International Affairs from Columbia University, a Master of Science in Technical Intelligence from National Intelligence University, and a B.A. in Philosophy and Psychology from Binghamton University.

## INTRODUCTION

As the United States (US) endeavors to establish international norms in cyberspace, it is critical that it delineate which behavioral norms it supports, how it plans to establish them, and to what ends the norms serve. These considerations are particularly timely as the current US administration builds its cybersecurity team and considers pressing issues in cyberspace. In January 2021, President Joe Biden appointed National Security Agency Cybersecurity Director Anne Neuberger as Deputy National Security Advisor (DNSA) for Cyber and Emerging Technology in the National Security Council.<sup>[3]</sup> As reported then, “Neuberger will be responsible for coordinating the federal government’s cybersecurity efforts, with a likely emphasis on responding to a massive cyberespionage campaign carried out last year by suspected Russian hackers [referencing SolarWinds], which the government is still struggling to unravel.”<sup>[4]</sup> She has since been joined in the administration by Chris Inglis, National Cyber Director, and Jen Easterly, Director of Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).<sup>[5]</sup>

Although the SolarWinds breach was extensive, affecting roughly 100 companies and a dozen government agencies,<sup>[6]</sup> the breach itself was not a violation of international norms as the operation did not escalate beyond espionage.<sup>[7]</sup> As the US devises its cyber policy, it is imperative to distinguish between actions taken for counterintelligence purposes and actions taken to develop international norms in cyberspace. Espionage is not a violation of an international norm, and the US does not appear inclined to establish it as such. Espionage and counter-espionage are established behaviors that participants have tacitly agreed to undertake and assume their associated costs. Yet some espionage-associated behavior in cyberspace fall

outside these bounds; for example, the US takes exception to espionage conducted “with the intent of providing competitive advantages to companies or commercial sectors.”<sup>[8]</sup>

Current literature advocates for tacit bargaining, that is, behavioral actions and counter-actions, in developing normative behavior in cyberspace.<sup>[9]</sup> The dynamics of the 2015 U.S.-China Cyber Agreement, however, indicate two important considerations: first, the necessity of explicit bargains, such as international agreements, to support the formation of desired norms that help avoid costly escalatory spirals. Second, how a viable prospect of cooperation underpins the success of norm development. Furthermore, the potential impact of actions taken outside of cyberspace must be taken into account as they did lead to the cyber accord and at least the temporary cessation of the People’s Republic of China (PRC) offending activity in cyberspace.<sup>[10]</sup> These are critical considerations for the US cybersecurity team as they develop US cyber policy: ideally, one directed towards a robust US-led multilateral, whole-of-government approach to the development of norms in cyberspace.

## THE SITUATION

The US National Cyber Strategy published in 2018 envisions an open, reliable, and secure cyberspace, one that supports American prosperity, liberty, and security.<sup>[11]</sup> The key to realizing this vision is accepting cyber norms that “define acceptable behavior to all states and promote greater predictability and stability in cyberspace”<sup>[12]</sup> and that “attribute and deter unacceptable behavior in cyberspace.”<sup>[13]</sup> The accompanying 2018 Department of Defense (DoD) strategy emphasizes long-term strategic competition from the People’s Republic of China (PRC), which has “expanded that competition to include persistent campaigns in and through cyberspace that pose long-term strategic risk to the Nation as well as to our allies and partners.”<sup>[14]</sup> The DoD strategy further notes that, “China is eroding US military overmatch and the Nation’s economic vitality by persistently exfiltrating sensitive information from US public and private sector institutions.”<sup>[15]</sup>

Aligning National Cyber Strategy goals with DoD’s characterization of the threat requires an assessment of unacceptable PRC behavior. It is critical to note that DoD characterized PRC’s espionage as the persistent exfiltration of sensitive information, which sought to damage US interests: through the erosion of US military overmatch and the erosion of US economic vitality.

Eroding US military overmatch is obviously a serious concern, but espionage with the intent to understand and neutralize military advantages has been accepted normative behavior since at least as early as Sun Tzu in the 5<sup>th</sup> Century, BCE.<sup>[16]</sup>

It is not espionage itself that is the relevant issue here; rather, it is the intent to erode US economic vitality. This is precisely the issue that President Obama raised with President Xi in the 2015 agreement: espionage “with the intent of providing competitive advantages to companies or commercial sectors,”<sup>[17]</sup> hereafter referred to as intellectual property-theft (IP-theft).

The 2015 U.S.–China Cyber Agreement states that “the United States and China agree that neither country’s government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.”<sup>[18]</sup> The parties also pledged to investigate and mitigate malicious cyber activities emanating from their respective territories, and to support development of “appropriate norms of state behavior in cyberspace.”<sup>[19]</sup> Post-agreement, similar agreements were made between the PRC and other G-20 members.<sup>[20]</sup> Yet the PRC’s active theft of IP have since continued.<sup>[21]</sup>

Continued IP theft has led Dr. Michael P. Fischerkeller of the Institute for Defense Analyses and Dr. Richard J. Harknett of the University of Cincinnati to argue that explicit bargaining, which involves “international conference or bilateral diplomacy and treaty negotiations,”<sup>[22]</sup> has significant limitations in the cyber domain because participants would not “trust the other to any agreement explicitly reached.”<sup>[23]</sup> They write:

Consider, for example, the 2015 agreement Presidents Obama and Xi, which committed that neither country would conduct or knowingly support cyber-enabled theft of intellectual property for commercial gain. ... This explicit agreement failed not because of any deficit in U.S. diplomatic bargaining skills, but because the bargaining process itself was not appropriate for the strategic competitive space to which it was applied.<sup>[24]</sup>

Instead, Fischerkeller and Harknett urge the use of tacit bargaining to develop normative behavior in cyberspace. Tacit bargains are defined by Schelling as “informal agreements arrived at ‘not by verbal bargaining, but by maneuver, by actions, and by statements and declarations that are not direct communication to the enemy.’”<sup>[25]</sup>

It is important to recognize that these two processes are not mutually exclusive. If the US had responded to violations of the U.S.–China Cyber Agreement<sup>[26]</sup> with more than mere words,<sup>[27],[28],[29]</sup> for example, with palpable actions against IP-theft recipients, the accord may have established an international norm and deterred future transgressions. Moreover, responses would not have had to be constrained to cyberspace: threat of economic sanctions is what compelled the PRC to enter into the accord in the first place.<sup>[30]</sup> Failure of the explicit bargain was not due to any structural realities of cyberspace, but, rather, to “Cheap Talk;”<sup>[31]</sup> the underlying potential payoffs for the PRC decision calculus ran counter to the explicit agreement. Xi had reason to convince Obama that it was in the PRC’s interests and intentions to respect IP, yet the PRC’s benefits from violating the agreement outweighed the prospective marginal cost, particularly if the prospect of US follow-through on the threat of sanctions diminished. As US enforcement of the agreement lagged,<sup>[32]</sup> the prospect of punishment diminished, and the calculus shifted in favor of IP-theft. Alternatively, the PRC may have perceived the prospective value of economic cooperation diminishing, given difficult trade negotiations throughout 2017–2018.<sup>[33]</sup> Either way, if actors are believed to be rational, trust in the agreement failed because interests were no longer aligned. The take away lesson should have been to enforce agreements, not necessarily that new interactions<sup>[34]</sup> in cyberspace are required to develop norms.

## WHY EXPLICIT BARGAINING IN CYBERSPACE IS NECESSARY

These new interactions, in the form of tacit bargaining, have become embodied in DoD's 2018 Cyber Strategy as a way to contest malicious cyber activity. Countering "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."<sup>[35]</sup> As Fischerkeller and Harknett explain it:

By describing *persistent engagement*, operationally, as continuously engaging and contesting adversaries and maneuvering for advantage below the threshold of armed conflict ... it is reasonable to conclude that persistent engagement would support a strategic process of tacit bargaining adopted to develop mutual understandings with adversaries on acceptable/unacceptable behavior in agreed competition.<sup>[36]</sup>

Notionally, then, U.S. Cyber Command (USCYBERCOM) would engage and contest adversaries conducting espionage in cyberspace for economic gain and thereby counter with consequences this unacceptable behavior. However, tacit bargaining in foreign networks, absent explicit bargains, risks establishing stable yet undesirable normative behavior.<sup>[37]</sup> Instead of the "open, reliable, and secure" cyberspace envisioned by the US strategy, this risks leaving the US vulnerable to costly escalatory spirals.

### *Escalatory Spirals*

Escalatory spirals spawned by cyberspace actions have already occurred. Examples include Iran accelerating its cyber development and deployment following the attack on its uranium enrichment centrifuges (Stuxnet attack<sup>[38],[39]</sup>), and Russia's claim that it was simply responding in kind through cyber means to the Panama papers release.<sup>[40]</sup> Predicated on whether cyberspace becomes truly offense-dominant or defense-dominant as the domain matures,<sup>[41]</sup> two types of escalatory spirals may occur in cyberspace:

- 1) A spiral that leads to a standoff with the potential to breach the limits of "competition short of armed conflict"<sup>[42]</sup>
- 2) A spiral that stabilizes as marginal costs eventually match marginal gains in a costly competition.<sup>[43]</sup>

In either case, at least in regards to IP-theft, both of these options are less desirable than a US-PRC agreement to reciprocate on IP protection and cooperate on combating the economic threat of cyber-crime which was the envisioned state of relations in the 2015 accord.

In lieu of an explicit agreement, consider if USCYBERCOM had engaged in tacit actions to punish and thereby compel the PRC to cease its IP-theft. US experience with economic sanctions has proven the importance of focusing efforts on the appropriate targets and communicate the desired behavior change.<sup>[44]</sup> As such, USCYBERCOM's two likely targets would be

- 1) Those who authorize and conduct state espionage in cyberspace, as well as the abetting network infrastructure (PRC cyberspace state espionage)
- 2) Those that receive and exploit the stolen IP (IP-theft recipients).

### ***Targeting PRC cyberspace state espionage***

While disrupting or degrading the PRC’s IP-theft enabling infrastructure is appealing, this approach is likely to be unhelpful for norm formation because the US is faced with a “Cheap Talk” dilemma of its own. This is because the US is motivated to disrupt or degrade this target for counterintelligence against espionage writ-large.<sup>[45]</sup> Even if explanatory communications accompany the counter-action and give IP-theft as the reason why it was imposed, there is no reason for the PRC to trust that these actions would end as the US benefits from the disruption. Furthermore, as the PRC would most likely not resume espionage from a network that is known to be compromised, there is no value proposition for the PRC to have the US cease its disruption or degradation activities. This is the antithesis for driving desired behavior change since it is necessary that the adversary sees both the prospect and value in the punishment ending when the egregious IP-theft behavior ends.<sup>[46]</sup> Tacit bargaining in this situation exacerbates the trust dilemma, not alleviates it. Instead, the US incurs ongoing manpower and resource costs to defend forward in order to suppress IP-theft, and the US and PRC are embroiled in an escalatory spiral in pursuit of marginal advantages over each other. As such, tacit bargaining, even with explanatory communications, contributes little to the development of the desired norm.

If the US could effectively disable all PRC espionage, that would eliminate IP-theft, but that is unrealistic. Again, the Iranian response to Stuxnet shows that an escalatory spiral is invariably in the offing given the low barrier to entry into cyberspace.<sup>[47]</sup> Even DoD acknowledges the futility of attempting to achieve total dominance.<sup>[48]</sup>

### ***Targeting IP-theft recipients***

Turning to the second set of targets, the *IP-theft recipients*, the US has followed “a two-pronged approach to combat economic espionage: (1) reducing theft by educating and training the private sector how to improve security and safeguard secrets,<sup>[49]</sup> and (2) federally prosecuting offenders.”<sup>[50]</sup> This latter approach has yielded a mixed bag<sup>[51]</sup> with few convictions under the 1996 Economic Espionage Act,<sup>[52]</sup> none involving cyber espionage. Considering that IP-theft continues to plague the US at enormous scale,<sup>[53]</sup> prosecuting offenders does not seem to have effectively stemmed or deterred cyber-enabled IP-theft, anecdotal arguments to the contrary notwithstanding.<sup>[54]</sup> Whether US actions targeting non-cyber actors, including the Department of Justice’s recently concluded China Initiative,<sup>[55]</sup> are successful at reducing espionage is outside the scope of this article.

A potential third US option is to threaten US cyberspace retaliation against businesses that exploit stolen US IP. This is likely to have some deterrent effect on IP-theft recipients' behavior. Examples of such potential punitive actions abound, from denial-of-service attacks against network infrastructure to malware akin to NotPetya<sup>[56]</sup> or high-profile ransomware attacks.<sup>[57]</sup> However, without an explicit bargain, these actions invite tit-for-tat reciprocal responses against US economic targets. Even if we assume that attribution for these actions makes them discernible from the background noise of cybercrime, without an explicit bargain, any US claim to legitimacy for its tacit actions is severely weakened, especially considering these actions would be conducted on foreign networks outside of US sovereignty. This greatly diminishes the value to normative behavior formation and lowers the barrier for retaliatory PRC action. Absent the explicit agreement, the PRC can simply claim the US violated their sovereign networks and reciprocate in kind. As such, prosecuting this target set with tacit actions in cyberspace also carries the potential for an escalatory spiral, not unlike the current US-PRC trade-war. The solution must include consideration for PRC domestic enforcement, which manifests in the prospect for cooperation discussed later herein.

### ***Prospect of Punishment and Retaliation***

Tacit bargains without explicit bargains risk escalatory spirals; explicit bargains need to be enforced. Had USCYBERCOM and other US agencies acted in defense of the 2015 U.S.–China Cyber Agreement by imposing punitive actions in response to PRC transgressions, this punishment would have helped to deter future transgressions.<sup>[58]</sup> Even Fischerkeller and Harknett support the dual importance of explicit and tacit bargains when they advocate for “an aligned application of them to the strategic realities the United States faces.”<sup>[59]</sup> They write further:

The success of a strategic framework for constructing cyber norms grounded in persistent engagement and tacit bargaining will depend, in part, on how well states communicate their national interests in cyberspace. Behavioral convergence around definable limitations is how sustainable cyber norms can be constructed.<sup>[60]</sup>

Those communicated defined limitations are the basis for explicit bargains, which confer legitimacy on retaliatory action; the prospect of retaliatory action and ensuing escalatory spirals supports behavioral convergence. This is where we see the convergence of explicit and tacit bargains. Even in the relatively benign costly competition scenario, the level of competition tacit bargaining will spawn will always be less desirable than a cyberspace characterized by cooperation. The US's failure to respond to PRC violations unfortunately, but predictably, emboldened PRC exploitation. However, while it becomes evident that explicit bargains and tacit enforcement are both necessary, this argument also leads to another question in the shadow of a potential escalatory spiral: what happens if the PRC reciprocates in kind against punishment, despite an explicit bargain? This question highlights the importance of the prospect of cooperation.

## **WHY CULTIVATING TRUE COOPERATION IS KEY**

Criminal, non-state sponsored, activity withstanding, why would the PRC choose to violate an explicit bargain in the face of a credible threat of retaliation? Assuming a rational actor, it would be simply because the prospective marginal gains still outweigh the prospective marginal costs. Though explicit bargains set the conditions for avoiding escalatory spirals, there must exist a viable and mutually beneficial solution which is attainable through the prospect of cooperation. Otherwise, both sides would be resigned to a future of escalatory standoffs or costly competition. Notably, this is where the dynamics of counter-intelligence and norm development diverge. Namely, espionage and counterintelligence have no other prospective solutions outside of tacit bargaining, absent the possibility of an intelligence-sharing treaty like the United Kingdom – United States of America Agreement (UKUSA), also known as the “Five Eyes.” Without such agreements, practitioners typically accept costly competition and retrospectively define the boundaries of acceptable action by triggering escalatory standoffs. Whether the SolarWinds hack is such a trigger or just becomes another aspect of costly competition remains to be seen. Either way, on norm development, it may be easier to build cooperation on economic issues as the market may have already provided the prospect for such regarding IP-theft.

In his seminal work, *The Evolution of Cooperation*, Robert Axelrod notes that the prospect of continued engagement enables cooperation to develop; inversely, a perception that the PRC or US would soon collapse undermines motivation for either party to cooperate. Instead, each would simply exploit the other for as much as it can steal from the other before the game ends. Assuming neither party is on the verge of collapse, in an environment in which continuous engagement is to be expected, for a strategy to be collectively stable—that is, able to resist the invasion of competing strategies—the strategy must offer a higher rate of return than a competing strategy. In other words, an international normative behavior must essentially be self-reinforcing. This requires two sequential conditions:

- 1) The reciprocal benefits of IP protections must be more beneficial amongst cooperating parties, e.g. the like-minded nations in the G-20, than for them to participate in IP-theft against each other
- 2) For (1) to be true, those who protect and respect IP must be prepared to retaliate collectively against those that adopt IP-theft, to deny, reduce, or otherwise render prohibitively costly the stolen IP.<sup>[61]</sup>

In essence, retaliation for violations of an international norm should be multilateral. Not only would a multilateral effort relieve the US of solely bearing the costs of enforcement, multilateral condemnation of IP-theft would provide even greater legitimacy to any punitive actions inside or outside cyberspace, raising the credibility and scope of potential punishment for violations while constraining the PRC’s freedom of action to retaliate in kind.

While effective retaliation may deter future transgressions, the ability to return to a mutually cooperative state is as important.<sup>[62]</sup> Pundits may argue that communicating on such intentions

is impossible due to issues of trust, but the economic market for justice may well have already provided the tacit evidence necessary to move nations and other entities towards a cooperative cyberspace and away from IP-theft. As Fareed Zakaria put it,

That China engages in rampant theft of intellectual property is a widely accepted fact—except among U.S. companies doing business in China. In a recent survey of such companies conducted by the U.S.-China Business Council, intellectual property protection ranked sixth on a list of pressing concerns, down from number two in 2014. ...Why this shift from 2014? That year, China created its first specialized courts to handle intellectual property cases. In 2015, foreign plaintiffs brought 63 cases in the Beijing Intellectual Property Court. The court ruled for the foreign firms in all 63.<sup>[63]</sup>

Since then, the IP caseload has grown rapidly. “In 2018 alone, Chinese courts received 301,278 new IP cases in the first instance, of which 287,795 were concluded. These figures represent an increase of 41 percent and 42 percent respectively compared to those for 2017.”<sup>[64]</sup> These include cases involving myriad American, Chinese, and other international companies.<sup>[65]</sup> Interestingly, ~79% of the cases brought before the court were purely PRC domestic cases,<sup>[66]</sup> with the remainder having foreign interests represented. In those latter cases, the court ruled in civil cases ~68% of the time in favor of foreign interests over domestic parties.<sup>[67]</sup>

Historical evidence points towards potential cooperation on intellectual property rights as well. As Yukon Huang and Jeremy Smith from the Carnegie Endowment for International Peace argue,

In terms of outright theft of IP, China’s infractions are anything but unique: It is just one of 36 violators listed in the 2019 Special 301 Report by the Office of the U.S. Trade Representative (USTR). Historically, rapidly growing emerging market economies tend to be cited as they transition to higher income levels. For example, decades ago Japan, South Korea, and Taiwan were each perennial Section 301 violators until they reached a per capita GDP of about \$20,000-\$25,000.<sup>[68]</sup>

Given the PRC’s per capita GDP is roughly \$17,000 as of 2020,<sup>[69]</sup> this hypothesis will likely be tested in the near future.

Others are less optimistic about China’s IP-theft, noting that the US Trade Representative cites numerous cases and complaints in the office’s 2018 report on PRC IP-theft.<sup>[70]</sup> And Zakaria does not consider that many affected US businesses may be unaware that they were victims of such theft.<sup>[71]</sup> However, Zakaria does highlight the convergence of PRC interests, US pressure, and desired normative behavior by stating that,

reforms...are often undertaken only in the face of Western pressure and, even then, because they serve China’s own competitive interests—the largest filer of patents worldwide last year was the Chinese telecommunications giant Huawei. But it is also true that many Chinese economists and senior policymakers have argued that the country will modernize and grow its economy only if it pursues further reform.<sup>[72]</sup>

While it may not be immediate, there certainly appears to be a prospect of cooperation that benefits both parties as the marginal gains from reciprocal IP protection outweigh the marginal gains from IP-theft as China’s economy matures.

Some claim that this was a *fait accompli*, that the Chinese economy was essentially able to mature because of the IP-theft over these past decades. This is perhaps true and it may have been a strategic failure of the US for not timely countering. However, it was not a failure of the US to envision an operational approach to cyberspace; tacit bargains without explicit bargains are unlikely to have been helpful; and tacit bargains in support of the explicit bargain, though some may have been potentially successful, would still run the risk of an escalatory spiral absent a perceived prospect of cooperation. Additionally, a multilateral effort to collaborate on punishing IP-theft and protecting the value of cybersecurity cooperation is still lacking. How to resolve the issues of retribution for past transgressions is beyond the scope of this article, which seeks to highlight the dynamics at play and explain why explicit bargains, the prospect of cooperation, and multilateral coordination outside of the cyberspace domain are important keys to developing international norms within cyberspace.

## **CONCLUSION**

The US government has an absolute obligation to keep its citizenry safe and uphold security commitments to allies and partners, and this article should not be read to suggest otherwise, or that the US should not contest espionage or protect sensitive technology that supports US security through military overmatch. However, in forming *desired* normative behavior, the focus is not the act of espionage itself, but the subsequent exploitation of the stolen IP. Tacit bargaining and actions alone are insufficient to develop this norm, and should be conducted in tandem with explicit bargains and a prospect of cooperation that is viable and desirable.

Following the 2015 U.S.–China Cyber Agreement, had USCYBERCOM imposed costs on PRC economic targets in response to transgressions, the explicit bargain might well have been saved through tacit enforcement, provided that prospective gains from cooperation and losses from a potential escalatory spiral were perceived as outweighing marginal gains from IP-theft. Given that the PRC is now exhibiting a willingness to retaliate against trade sanctions in a reciprocal manner, unfettered tacit actions in cyberspace seem more likely than ever to trigger a retaliation rather than establish deterrence. This is evidenced by the PRC’s recent passage of its Anti-Foreign Sanctions Law which legalizes PRC retaliation against companies complying with US and EU sanctions.<sup>[73]</sup> Perhaps the most compelling, and ironic, example against the standalone use of tacit bargaining in cyberspace is the PRC actions following the 2015 accord. US officials were left befuddled as to why the PRC decided to renege on its commitments<sup>[74]</sup> and PRC actions have clearly provoked further US escalatory responses, leading to an escalatory spiral in the tit-for-tat trade war. Whether the trade war results in a stable costly competition centered on reciprocal tariffs, an escalatory standoff threatening military action, or a return to the liberalization of trade remains to be seen.

In addition to the appointments of the Deputy National Security Advisor for Cybersecurity to the National Security Council, the National Cyber Director, and the Director for CISA, the Department of State recently established the Bureau of Cyberspace and Digital Policy (CDP) to lead US government diplomatic efforts on: (1) International cybersecurity focusing on deterrence, negotiations and capacity building, (2) International digital policy for internet governance and trust in global telecom systems, and (3) Digital freedom in regards to human rights and engagement between the private sector and society.<sup>[75]</sup> This raises the prospect for coordinating a multilateral approach to dealing with IP-theft. As Axelrod's analysis suggests, all cooperating entities on a norm should retaliate against violators in support of collective stability.<sup>[76]</sup> Regarding IP-theft, as Richard McGregor writes, traditional US allies and partners like Europe, Australia, and Japan are eager to work more closely with the US on China trade policy.<sup>[77]</sup> The opportunity may be at hand, through multilateral collaboration, to enhance the legitimacy of any punitive actions for IP-theft while constraining the PRC's freedom of action for retaliatory actions in kind. This is particularly pertinent given that the PRC already has standing explicit agreements on IP-theft with G-20 countries.

Rather than limiting itself to cyberspace alone, the US should also leverage tools and levers across the US government to change expected value propositions for PRC actions; a whole of government approach. Clearly, actions outside the cyberspace domain influence actions within it: note again that it was the prospect of economic sanctions that motivated the PRC to enter into the 2015 Accord in the first place. Much work remains to be done on formulating US cyber policy and how the US chooses to align interests and actions in cyberspace. However, we should hope that the prospect of cooperation remains viable, lest we resign ourselves to the constant risk of escalatory spirals. As the new US national cybersecurity leadership establishes themselves, the US has an opportunity to revisit explicit bargains and foster multilateral cooperation on tacit actions.♥

## **DISCLAIMER**

The views expressed here are the author's and do not necessarily reflect the position of the National Intelligence University, the U.S. Army Reserve 75th Innovation Command, the Department of Defense, the U.S. Intelligence Community, or the U.S. Government.

## **ACKNOWLEDGEMENTS**

This article was based on my thesis at National Intelligence University, and I would like to thank my advisors, Professor Jason Healey, Columbia University, and Lieutenant Colonel John Duselis, U.S. Marine Corps. I would also like to thank Vivian Lei, my wife, for her enduring support.

## NOTES

1. The broadest definition of an upper bound for acceptable behavior of operations in cyberspace in peacetime are those that fall short of the “scale and effects” attributed to the “use of force,” drawing its verbiage from the UN Charter, Article 2(4). International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations*, Edited by Michael N. Schmitt and Liis Vihul, (New York: Cambridge University Press, 2017), 339.
2. Office of the Press Secretary, The White House, “Fact Sheet: President Xi Jinping’s State Visit to the United States,” September 25, 2015, <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states>, accessed on July 30, 2020.
3. William Turton, “The Former NSA Official Vying to Steer Biden’s Cyber Policy,” January 7, 2022, <https://www.bloomberg.com/news/articles/2022-01-07/anne-neuberger-the-former-nsa-official-shaping-biden-s-cybersecurity-policy>, accessed on January 17, 2022.
4. Natasha Bertrand, “Biden taps intelligence veteran for new White House cybersecurity role,” *Politico*, January 6, 2021, <https://www.politico.com/news/2021/01/06/biden-white-house-cybersecurity-neuberger-455508>, accessed on January 18, 2021.
5. Ellen Nakashima, “Biden administration plans to name former senior NSA officials to White House cyber position and head of CISA,” April 12, 2021, [https://www.washingtonpost.com/national-security/former-senior-nsa-officials-named-to-white-house-cyber-position-and-head-of-dhs-cyber-agency/2021/04/11/b9d408cc-9b2d-11eb-8005-bffc3a39f6d3\\_story.html](https://www.washingtonpost.com/national-security/former-senior-nsa-officials-named-to-white-house-cyber-position-and-head-of-dhs-cyber-agency/2021/04/11/b9d408cc-9b2d-11eb-8005-bffc3a39f6d3_story.html), accessed January 17, 2022.
6. Dina Temple-Raston, “A ‘Worst Nightmare’ Cyberattack: The Untold Story Of The SolarWinds Hack,” April 16, 2021, <https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack>, accessed on September 9, 2021.
7. Michael Schmitt, “Top Expert Backgrounder: Russia’s SolarWinds Operation and International Law,” Just Security, December 21, 2020, <https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/>, accessed on January 17, 2022.
8. Office of the Press Secretary, The White House, “Fact Sheet: President Xi Jinping’s State Visit to the United States,” September 25, 2015, <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states>, accessed on July 30, 2020.
9. Michael P. Fischerkeller and Richard J. Harknett, “Persistent Engagement and Tacit Bargaining: A Path Toward Norms in Cyberspace,” *Lawfare*, November 9, 2018, <https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace>, accessed on July 20, 2020.
10. John P. Carlin and Garrett M. Graff, *Dawn of the Code War: America’s Battle Against Russia, China, and the Rising Global Cyber Threat*, (New York, NY: PublicAffairs, 2018.)
11. The White House, “National Cyber Strategy,” 2018, <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>, accessed on August 6, 2020.
12. *Ibid*, 20.
13. *Ibid*, 21.
14. Department of Defense, “Cyber Strategy Summary,” 2018, 1, [https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER\\_STRATEGY\\_SUMMARY\\_FINAL.PDF](https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF), accessed on July 30, 2020.
15. *Ibid*.
16. Mike Giglio, “China’s Spies Are on the Offensive,” *The Atlantic*, August 26, 2019, <https://www.theatlantic.com/politics/archive/2019/08/inside-us-china-espionage-war/595747/>, accessed on July 30, 2020.
17. Office of the Press Secretary, The White House, “Fact Sheet: President Xi Jinping’s State Visit to the United States,” September 25, 2015, <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states>, accessed on July 30, 2020.
18. *Ibid*.
19. *Ibid*.
20. Adam Segal, “The U.S.-China Cyber Espionage Deal One Year Later,” Council on Foreign Relations, September 28, 2016, <https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later>, accessed on July 30, 2020.

## NOTES

21. National Counterintelligence and Security Center, “Foreign Economic Espionage in Cyberspace,” 2018, <https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf>, accessed on July 30, 2020.
22. Fischerkeller and Harknett, “Persistent Engagement and Tacit Bargaining.”
23. Ibid.
24. Ibid.
25. Ibid.
26. Fireeye, “Redline Drawn: China Recalculates its use of Cyber Espionage,” June 2016, <https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf>, accessed on August 6, 2020.
27. Cory Bennett, “Why Trump is sticking with Obama’s China hacking deal,” *Politico*, November 8, 2017, <https://www.politico.com/story/2017/11/08/trump-obama-china-hacking-deal-244658>, accessed on July 20, 2020.
28. Chris Bing, “Trump administration says China broke Obama-Xi hacking agreement,” *cyberscoop*, March 22, 2018, <https://www.cyberscoop.com/trump-china-hacking-obama-xi-agreement/>, accessed on August 6, 2020.
29. Department of Homeland Security, “First U.S.-China Law Enforcement and Cybersecurity Dialogue,” October 6, 2017, <https://www.dhs.gov/news/2017/10/06/first-us-china-law-enforcement-and-cybersecurity-dialogue>, accessed on August 6, 2020.
30. Carlin and Graff, *Dawn of the Code War*, 366-367.
31. Joseph Farrell and Matthew Rabin, “Cheap Talk,” *Journal of Economic Perspectives*, Vol. 10.3 (1996), 103-118.
32. Carlin notes that there was a “new norm” that had broken down by 2018. He does not detail any US response except that of Jeff Session’s China Initiative starting in 2018. John P. Carlin and Garrett M. Graff, *Dawn of the Code War: America’s Battle Against Russia, China, and the Rising Global Cyber Threat*, (New York: PublicAffairs, 2018), 370.
33. Heather Timmons, “Timeline: Key dates in the U.S.-China trade war,” *Reuters*, January 15, 2020, <https://www.reuters.com/article/us-usa-trade-china-timeline/timeline-key-dates-in-the-u-s-china-trade-war-idUSKBNIZE1AA>, accessed on August 6, 2020.
34. Michael P. Fischerkeller and Richard J. Harknett, “Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation,” *Institute for Defense Analysis*, May 2018, 9, <https://www.ida.org/-/media/feature/publications/p/pe/persistent-engagement-agreed-competition-cyberspace-interaction-dynamics-and-escalation/d-9076.ashx>, accessed on July 30, 2020.
35. Department of Defense, “Cyber Strategy Summary,” 2018, 4, [https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER\\_STRATEGY\\_SUMMARY\\_FINAL.PDF](https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF), accessed on July 30, 2020.
36. Fischerkeller and Harknett, “Persistent Engagement and Tacit Bargaining.”
37. Akin to a suboptimal Nash equilibrium in a continuous Prisoner’s Dilemma - Pareto efficient outcomes that are undesirable compared to other pareto efficient outcomes that have higher payoffs; Colin F. Camerer, *Behavioral Game Theory: Experiments in Strategic Interaction* (Princeton, New Jersey: Princeton University Press, 2003).
38. Following the 2010 Stuxnet attack against Iran’s uranium enrichment centrifuges, Iran has since developed and employed offensive cyber attack capabilities. Andrea Shalal-Esa, “Iran strengthened cyber capabilities after Stuxnet: U.S. general,” *Reuters*, January 17, 2013, <https://www.reuters.com/article/us-iran-usa-cyber-idUSBRE90GIC420130118>, accessed on July 30, 2020.
39. Congressional Research Service, “Iranian Offensive Cyber Attack Capabilities,” January 13, 2020, <https://sgp.fas.org/crs/mideast/IF11406.pdf>, accessed on September 9, 2021.
40. “Putin publicly pointed to the Panama Papers disclosure...as US-directed efforts to defame Russia...” and is assessed to be a potential driver for Russia’s interference in the 2016 US Presidential Election. Office of the Director of National Intelligence, “Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections,” January 6, 2017, [https://www.dni.gov/files/documents/ICA\\_2017\\_01.pdf](https://www.dni.gov/files/documents/ICA_2017_01.pdf), accessed on July 30, 2020.
41. Concepts of offense- and defense-dominant from Robert Jervis; Robert Jervis, “Cooperation under the Security Dilemma,” from *Conflict After the Cold War: Arguments on Causes of War and Peace, 5th Edition* edited by Richard Betts, (New York, NY: Routledge 2017).
42. Fischerkeller and Harknett, “Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation,” 9.

## NOTES

43. Readers familiar with economic theory may recognize the similarity of this concept to suboptimal Pareto efficiencies derived from participants pursuing dominant strategies in a Prisoner’s Dilemma game.
44. Richard Nephew, *The Art of Sanctions: A View from the Field*. (New York: Columbia University Press, 2018).
45. National Counterintelligence and Security Center, “National Counterintelligence Strategy of the United States of America 2020-2022,” January 7, 2020, [https://www.dni.gov/files/NCSC/documents/features/20200205-National\\_CI\\_Strategy\\_2020\\_2022.pdf](https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf), accessed on August 6th, 2020.
46. Richard Nephew, *The Art of Sanctions: A View from the Field*. (New York: Columbia University Press, 2018).
47. Robert Jervis and Jason Healey, “The Dynamics of Cyber Conflict,” Columbia University, SIPA, August 2, 2019, <https://sipa.columbia.edu/sites/default/files/embedded-media/Brochure%20on%20the%20Dynamics%20of%20Cyber%20Conflict.pdf>, accessed on July 30, 2020.
48. USCYBERCOM, “Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command,” 2018, <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010>, accessed on July 30, 2020.
49. Passive defensive actions to “harden” potential economic targets of IP-theft are out of scope for this paper; however, there is evidence that such efforts have not been effective at stemming cyber-crime, let alone state-sponsored cyber espionage. Coveware, “Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound,” April 26, 2021, <https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound>, accessed on September 9, 2021.
50. Melanie Reid, “A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing with This Global Threat?” *University of Miami Law Review*, Vol. 70, No. 1 (2016), 58.
51. Andrew Boutros, David Kelley, and Jay Schleppebach, “Department of Justice Year-End Update Shows ‘China Initiative’ Prosecutions Are Alive and Well,” Dechert LLP, December 7, 2021, <https://www.jdsupra.com/legalnews/departments-of-justice-year-end-update-2087556/>, accessed on January 17, 2022.
52. Eileen Guo, Jess Aloe, and Karen Hao, “The US crackdown on Chinese economic espionage is a mess. We have the data to show it,” MIT Technology Review, December 2, 2021, <https://www.technologyreview.com/2021/12/02/1040656/china-initiative-us-justice-department/>, accessed on January 17, 2022.
53. The Commission on the Theft of American Intellectual Property, “Update to the IP Commission Report,” The National Bureau of Asian Research, 2017, [http://ipcommission.org/report/IP\\_Commission\\_Report\\_Update\\_2017.pdf](http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf), accessed on July 30, 2020.
54. Neal Pollard et. al., “Named But Hardly Shamed: The Impact of Information Disclosures on APT Operations,” Columbia University, SIPA Capstone Project, Spring 2020.
55. Department of Justice, “Attorney General Jeff Session’s China Initiative Fact Sheet,” November 1st, 2018, <https://www.justice.gov/opa/speech/file/1107256/download>, accessed on January 17, 2022. Steve Kwok, “DOJ Steps Back From China Initiative But Remains Focused On China-Related Enforcement,” Coventus Law, April 1, 2022, <https://coventuslaw.com/report/doj-steps-back-from-china-initiative-but-remains-focused-on-china-related-enforcement/>, accessed on April 15, 2022.
56. NotPetya was a high-profile malware attack that crippled infrastructure and organizations around the world that is assessed to have been originally directed at Ukraine by Russia, but went awry due to poor safeguards in the coding. Mike McQuade, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History,” Wired, August 22, 2018, <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>, accessed on July 30, 2020.
57. Matt Stieb, “What’s Driving the Surge in Ransomware Attacks?” *Intelligencer*, *New York Magazine*, June 11, 2021, <https://nymag.com/intelligencer/article/ransomware-attacks-2021.html>, accessed on June 13, 2021.
58. Joseph S. Nye, “Deterrence and Dissuasion in Cyberspace,” *International Security*, Vol. 41, No. 3, Winter 2016/2017, 44-71.
59. Michael P. Fischerkeller and Richard J. Harknett, “Persistent Engagement and Tacit Bargaining.”
60. Ibid.
61. Robert Axelrod, *The Evolution of Cooperation*: rev. ed. (New York: Basic Books, 2009).
62. Ibid.
63. Fareed Zakaria, “The New China Scare: Why America Shouldn’t Panic About Its Latest Challenger,” *Foreign Affairs*, Vol. 99, No. 1, 2020, 59.

## NOTES

64. Tao Kaiyuan, “China’s commitment to strengthening IP judicial protection and creating a bright future for IP rights,” *WIPO Magazine*, World Intellectual Property Organization, June 2019, [https://www.wipo.int/wipo\\_magazine/en/2019/03/article\\_0004.html](https://www.wipo.int/wipo_magazine/en/2019/03/article_0004.html), accessed on July 30, 2020.
65. Aaron Wininger, “China’s Supreme People’s Procuratorate Issues Top Example Cases of Criminal Intellectual Property Rights Infringement in 2019,” *The National Law Review*, Vol X. No. 212, April 26, 2020, <https://www.natlawreview.com/article/china-s-supreme-people-s-procuratorate-issues-top-example-cases-criminal>, accessed on July 30, 2020.
66. DEQI Intellectual Property Law Corporation, “Beijing Intellectual Property Court: Foreign-related Intellectual Property Cases Increasing Year by Year,” <https://www.lexology.com/library/detail.aspx?g=62f25070-8679-4b84-bf67-202b3109e949>, accessed on September 9, 2021.
67. *Ibid.*
68. Yukon Huang and Jeremy Smith, “China’s Record on Intellectual Property Rights Is Getting Better and Better,” October 16, 2019, <https://carnegieendowment.org/2019/10/16/china-s-record-on-intellectual-property-rights-is-getting-better-and-better-pub-80098>, accessed on September 9, 2020.
69. World Bank, “GDP per capita, PPP (current international \$) – China” Most recent year 2020, <https://data.worldbank.org/indicator/NY.GDP.PCAP.PP.CD?end=2020&locations=CN&start=1990>, accessed on September 9, 2020.
70. Office of the United States Trade Representative, Executive Office of the President, “Findings of the Investigation into China’s Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974,” March 22, 2018. <https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF>, accessed on July 30, 2020.
71. Megan Reiss, “Counting Cybercrimes,” *The American Interest* February 27, 2018, <https://www.the-american-interest.com/2018/02/27/counting-cybercrimes/>, accessed on July 30, 2020.
72. Zakaria, “The New China Scare: Why America Shouldn’t Panic About Its Latest Challenger,” 59.
73. Chun Hanong, “China Passes Law to Counter Foreign Sanctions,” *The Wall Street Journal*, June 10, 2021, <https://www.wsj.com/articles/china-passes-law-to-counter-foreign-sanctions-11623327432>, accessed on June 13, 2021.
74. David E. Sanger and Steven Lee Myers, “After a Hiatus, China Accelerates Cyberspying Efforts to Obtain U.S. Technology,” *The New York Times*, November 29, 2018, <https://www.nytimes.com/2018/11/29/us/politics/china-trump-cyberespionage.html>, accessed on August 6, 2020.
75. Samantha Schwartz, “State Department to add cyber bureay, tackle tech diplomacy,” November 9, 2021, <https://www.cybersecuritydive.com/news/state-department-to-add-cyber-bureay-tackle-tech-diplomacy/609697/>, accessed on January 17, 2022.
76. Robert Axelrod, *The Evolution of Cooperation*, rev. ed. (New York: Basic Books, 2009).
77. Richard McGregor, *Xi Jinping: The Backlash*, Lowy Institute for International Policy, (Docklands, Australia: Penguin Books, 2019).



# Timing Influence Efforts with Information Processing

---

Dr. Joshua McCarty  
Kaylee Laakso

**T**hanks to technological advancements and global connectivity, the information environment continues to evolve as new information channels emerge. However, despite evolutions in the information environment, the role and nature of information in people's lives have not changed. Even with the advent of social media, the internet, and other technologies that have increased access to information, two principles remain the same. The first principle is that people seek information to reduce the uncertainty associated with their perception of insufficient knowledge.<sup>[1]</sup> The second principle is that information processing is a social process.<sup>[2]</sup> These principles are explored within the context of timing to facilitate better effects from influence efforts that are sequenced and executed to maximize influence opportunities. The timing of target populations' information-seeking and socialization represents a window of opportunity for influence. As information is socialized and accepted, the attribution of this information becomes part of a shared reality and storied identity.<sup>[3]</sup>

The importance of message timing is not new, but the discernment of a clear window to exploit for influence purposes is. The window for exploitation is the period during which information seeking and socialization occur following a crisis. This period is pertinent to all influence practitioners in their timing of messages from initial exposure through socialization. The window of opportunity is relevant for a range of influence activities that include mass, precision, and deception, regardless of the information channel.

Within this window, if influence efforts can be connected to a plan, or a perceived solution to the event, the opportunity to leverage the focusing event for change increases. The golden hour rule in crisis response is intended to ensure people receive sufficient infor-



**Dr. Joshua McCarty** is a retired Army Psychological Operations Officer and currently serves as adjunct faculty in the Communication department with Purdue University Global and a PSYOP training specialist with 5th Battalion, 1st Special Warfare Training Group at Fort Bragg, North Carolina. He holds a Ph.D. in Communication Studies from Regent University and a Master of Arts from Seton Hall University in Strategic Communication and Leadership. McCarty has published in the *Journal of Media and Religion* in addition to numerous academic conference presentations. He developed the crisis opportunity model, which identifies how a crisis can be leveraged for social change. He also coauthored the deception opportunity model, which identifies the duration in which people are most vulnerable to deception. His specialties include crisis and uncertainty communication, religion and social media, crisis exploitation, narrative, and media effects.

mation and avoid turning to other sources or allowing rumors, disinformation, or misinformation to emerge. Delays in response can cause several issues, including loss of audience since they will likely turn to alternate sources. Amplifying the necessity for timely messaging, as time passes, audience reach lessens, and rumors emerge that require practitioners to expend more resources to overcome potential consequences of untimely messaging.

This research explores and discerns information processing durations for information seeking and socializing. The research consisted of an analysis of two published case studies, a third original case study, and the analysis of aggregated data from all three case studies. Based on previous research, the first case study traces information-seeking through support for a policy change that demonstrates the importance of timely messaging.<sup>[4]</sup> The second case study expands the findings of the first case study by examining the information-seeking behaviors of three additional crises with daily variables for a more accurate depiction of those behaviors. The third case study, based on previous research, examines the relationship of both information seeking and socialization behaviors in a crisis. The examination of the case studies in aggregate provides a holistic study of information processing behaviors after five crises, specifically illuminating the relationship and timing of information-seeking and socialization behaviors. It amplifies the salience of message timing in both information seeking and socialization. In addition to message timing, the study underscores that messages should be tailored to support the specific information processing window.

The framework of this study is from a communication perspective. It incorporates numerous theories, including uncertainty, the social construction of reality, crisis communication, and narrative. Uncertainty theories explain information processing during periods of



**Kaylee Laakso** is a former Army Psychological Operations Officer and current Ph.D. student in Rhetorics, Communication, and Information Design at Clemson University. She earned a Master of Professional Studies in Security and Safety Leadership from The George Washington University. Kaylee was a fellow with the Turkish Heritage Organization and published numerous articles on media and communication topics pertaining to U.S.-Turkish relations. She is a recognized expert in fake news and presented a TEDx Talk at Northern Michigan University. Kaylee also presented on disinformation as the keynote speaker at Tiffin University's virtual graduate conference. She coauthored the deception opportunity model identifying conditions and vulnerabilities that make audiences more susceptible to deception. She has led or participated in the research, planning, and project efforts in 13 countries across five continents. Her areas of specialization include deception, information operations, and social media manipulation.

stress. Information processing is what determines how people understand the world around them. A storyline or narrative emerges as people understand an event and connect it to other events. Influence practitioners who provide relevant information when and where the populace is seeking and socializing that information will more effectively influence how they view the world and subsequently perceive similar events in the future. In order to influence perceptions and behaviors, it is necessary to participate in the conversation as it takes place during both seeking and socialization.

Walter Fisher posited the third narrative paradigm, how a narrative is a rhetorical tool.<sup>[5]</sup> As people accept information that explains events around them, it shapes their understanding and the construction of their reality if the story rings true and holds together.<sup>[6]</sup> Stories subsume logic and reason and are judged on narrative rationality, including coherence and fidelity.<sup>[7]</sup> As a community socializes what an event means, a consensus will be reached. This consensus and the corresponding accepted meaning of the event then becomes a storied part of the community.

The challenge remains for influence practitioners to have a story accepted over other stories competing to explain the same event that supports their influence efforts. Messaging during information processing windows of opportunity increases the probability of an event being connected to themes supporting a narrative.

### *Literature Review*

Influence opportunities center on focusing events, which are sudden, relatively uncommon events that garner the interest and attention of the population.<sup>[8]</sup> Focusing events present opportunities for precisely influencing and deceiving the masses. Focusing events produce uncertainty that spurs information processing. A brief review of current literature includes crisis, uncertainty, social construction of reality, and narrative theories to provide a framework for this study.

### *Crisis*

A crisis is an unexpected, non-routine event or series of events that create high levels of uncertainty and a significant perceived or actual threat to goals such as obtaining education, acquiring wealth, or even maintaining family traditions.<sup>[9]</sup> Crises cause people to behave differently than they normally would.<sup>[10]</sup> They come in many forms, such as natural disasters, manufactured disasters, terrorist attacks, organizational catastrophes, or economic crises. The type of crisis may characterize the level of uncertainty the population is facing. The greater the number of people who experience high levels of uncertainty caused by a crisis, the more people there are to potentially seek information. It is then that people are more susceptible to malicious, adversarial, or even friendly influence efforts that can lead to behavioral and social change.

Crises cause uncertainty by creating an information void that is left to be filled by someone, somehow.<sup>[11]</sup> Uncertainty is stress, anxiety, discomfort, or a perceived threat that disorients one's abilities to properly appraise the situation and maintain a state or sense of rational order due to limited knowledge.<sup>[12]</sup> The information void caused by the crisis results in uncertainty as people seek to determine what the crisis means. Uncertainty causes people to ask questions about the event and how they view the world.

### *Focusing Event*

A focusing event is a catalyst for information seeking and socialization. Thomas Birkland considered a focusing event as an expansion of the definition of a crisis with additional criteria of concentrated harm in a community of interest and known simultaneously to both the public and the government.<sup>[13]</sup> Another aspect of Birkland's criteria is that a focusing event is relatively uncommon. It would be possible for a commonly occurring crisis to no longer be considered a focusing event as people would be desensitized to it.<sup>[14]</sup>

Focusing events are tied to issue attention cycles and policy change.<sup>[15]</sup> Focusing events often shift attention to the media and unattended or under-attended issues.<sup>[16]</sup> Increased coverage following a focusing event elevates issue enthusiasm, which results in agenda space for related issues.<sup>[17],[18]</sup> After such focusing events, people are looking for a plan of action and turn to relevant media or social structures to learn about plans.

Focusing events can result in identifying new problems or increasing the salience of a dormant issue, leading to possible solutions, especially when a crisis results from a perceived policy failure.<sup>[19]</sup> The process of linking focusing events to issues is done to frame the event to support an agenda.<sup>[20]</sup> Issue advocates may take advantage of the situation to redefine the issues connected with the event, aiding or exploiting the media in framing the event to current failures and calls for action.<sup>[21]</sup> In Nigeria, during significant drops in oil prices between 2011 and 2014, adversarial non-state actors framed the reduction in oil revenue distributions to the history of corruption when it was really the result of a drastic drop in oil prices.<sup>[22]</sup>

Even though it was not true, it seemed feasible given the perceived history of corruption; therefore, many in the population believed it.

Birkland and Schattschneider found that group efforts are essential for policy change as they increase the likelihood of more influential participants entering into a policy change discussion.<sup>[23],[24]</sup> Schattschneider considered group participation a form of pressure or intimidation using “something other than reason and information to induce public authorities to act against their own best judgment.”<sup>[25]</sup> Pro-change groups use media-generated symbols of a focusing event to dramatize and evidence a need for change.<sup>[26]</sup> A focusing event can shift the balance on an issue, especially when the issue advocates are well organized.<sup>[27]</sup> Organizations and social structures have policy agendas that shape how they communicate to the public and interact with media to maximize the opportunity a focusing event provides. Focusing events provide a “window of opportunity” for issue advocates to leverage curated messages and information channels for policy change.

### ***Information***

Information plays a significant role in addressing uncertainty. Numerous theories provide insights into understanding human nature and explain corresponding opportunities for influence. Uncertainty theories explain information-seeking behaviors intended to reduce stress and cognitively process uncertainty. Uncertainty presents when there is a perception of insufficient knowledge. Therefore, uncertainty can be reduced by ingesting information about the cause of uncertainty.<sup>[28]</sup> Knowledge and information allow people to develop meaning and understand an event as long as the information creates a sense of coherence.<sup>[29]</sup> A challenge is that there are many sources of information, and if the information is inadequate, the resulting void may be co-opted.<sup>[30]</sup> It is important to note that people are not simply looking for information but a story to manage cognitive and emotional demands.<sup>[31]</sup> Information alone can be insufficient to reduce uncertainty.<sup>[32]</sup> The significance of information and its role in reducing uncertainty drives people to employ information seeking strategies to meet their cognitive and emotional demands.

People often refer to what they consider to be previous, similar events to help make sense of and understand what current events mean. This behavior includes information seeking of similar, previous events as information about the current event may not initially be available. People look for information relevant to them that tells a story and provides understanding and meaning to the event related to their lives.<sup>[33]</sup> If the story coherently explains the event, aligning with their prior understanding and experiences, then that explanation will likely be accepted for socialization—collective information processing. People take different approaches to obtain information with four strategies that govern information-seeking behaviors.

### ***Information-Seeking Strategies and Behavior***

The theory of motivated information management considers individual motivation to seek

or avoid information that the individual deems important, resulting in action to adjust uncertainty.<sup>[34]</sup> Uncertainty motivates people to communicate by weighing outcome rewards and costs.<sup>[35]</sup> Motivation drives people's communication behavior.<sup>[36]</sup> Assessing reward versus cost influences the strategy selection, which in turn impacts behavior. Uncertainty alters people's plans, and when plans fail, people alter their approach in ways that require the least cognitive effort.<sup>[37]</sup>

There are four information-seeking strategies: passive, active, interactive, and avoidance. Information-seeking behavior manifests information-seeking strategies, which are actions to obtain more information or inactions to avoid information. A passive strategy includes behaviors that involve observations about the uncertainty-causing event to gain insight but not seeking out information. An active strategy includes behaviors that involve taking action to seek information, whether through traditional media or social networks. Interactive information-seeking includes behaviors that involve communication with others, especially with subject-matter experts who are likely the information source, such as a medical doctor, when a patient wants to learn the result of a blood test. Information avoidance is a deliberate effort not to encounter information related to the cause of uncertainty, often due to fear of what the information could be and the potential of greater uncertainty.

In this research, the case studies for information-seeking include only active and interactive information-seeking behaviors. The case study on information-socialization includes interactive, active, and passive information-seeking behaviors. Information socialization allows the information sought from one's social network to reach passive information seekers and potentially influence their attitudes and behaviors.

### ***Information Socialization***

Information gathering is a social process.<sup>[38]</sup> Interaction and communication about the information is a process of creating shared meaning between people, groups, and communities.<sup>[39]</sup> People engage in collaborative information-seeking to resolve a shared information need.<sup>[40]</sup> When people are confronted with stress and uncertainty, they seek support from social structures and processes they built.<sup>[41]</sup> These social structures include family, friends, social networks, religious institutions and communities, and government. People emotionally crave assurance through dyadic coping to find support, additional information, tools, and keys to decode reality.<sup>[42]</sup>

As people engage with other people, they engage in coping and coordinated problem solving with the available information.<sup>[43]</sup> As people engage, they experience a sense of clarity and certainty from identifying with a collective.<sup>[44]</sup> The structures and social networks people seek support from become a filter of information, providing the information deemed necessary and suited to their perspective. The result is that the collective network shares a common lens to interpret and appraise uncertainty based on shared values and beliefs. The socialization period

increases people's susceptibility to new ideas, misinformation, deception, disinformation, and other influence efforts. The information has already passed through one filter to make it to the socialization stage. The information will be judged based on who presented the information to the social group.

### ***Social Construction of Reality***

A common lens and shared sense of reality is the result of the construction of human knowledge through social interaction, as posited by Peter Berger and Thomas Luckmann.<sup>[45]</sup> Social construction of reality explores how meaning develops with others. Each group develops meaning and understanding of the world particular to them. The theory of constructionism is how people interact and develop the meaning of events or a social reality. The social reality formulates an interpretative schema for future, similar events. Understanding an audience's interpretative schemes and categorization of previous events can shape persuasive efforts by building on those schemes to influence the interpretation of future events. The ability to influence this approach is from Walter Fisher's Third Narrative Paradigm. Using a narrative as a rhetorical tool, a storied approach of unfolding events provides the needed explanation and meaning. If the narrative is persuasive and socialized, it can inform the construction of human knowledge through social interaction.

A narrative used for persuasive efforts is driven by events, similar events that build a storyline and plot that supports the need for and propels change. A consistent explanation of multiple events within a storyline, a series of events, results in narrative rationality. Narrative rationality is the coherence and fidelity of a narrative—the extent a story hangs together and rings true.<sup>[46]</sup> It is how the media and news guide people in understanding their world. The narrative can be a powerfully persuasive tool if it can reach its intended audience and be accepted by their social network during socialization. The story is the primary mode of deception. It can also aid in persuading people to take actions aligned with a narrative by amplifying issues and events related to a theme and providing a plan of action.

The narrative as a rhetorical tool is powerful, but it needs to engage people during the windows of opportunity. Three case studies are explored to understand the windows of opportunity and the duration people engage in active and interactive information seeking.

### ***Case Study 1: A Window of Opportunity for Information Seeking***

The crisis opportunity model (COM) examined the relationship between a crisis, its media coverage, how media sources covered the crisis and public opinion on issues connected to the crisis.<sup>[47]</sup> The study also examined people's information-seeking tendency following a crisis to fulfill their need for orientation. The crisis in this study was the Sandy Hook school shooting. The study found that people ask questions and seek information for about two weeks, confirming the two-week window in another study that examined behavior following the September 11th, 2001 terrorist attack.<sup>[48]</sup> The COM study collected and examined the variables every

week. The study resulted in a model that identified significant relationships between people’s information seeking, media coverage of a crisis, and changes in support for policy change.

Information-seeking provided the path to change. The media amplified the need for change by including coverage of previous shootings as evidence. The study found significant relationships between the media coverage of the crisis with references to previous events and support for change with one exception. The shooting in Tucson, Arizona, did not result in a significant relationship with support for change. Upon further examination, the Tucson media coverage began a full month after the Sandy Hook shooting, while the media coverage of other previous shootings occurred within the initial two weeks following the crisis. This case study provided evidence that messaging within the window of opportunity influenced public opinion, and coverage after this time did not. The study’s implications indicate that the Tucson media coverage was outside the information socialization period. The data structure limited the sensitivity to weekly periods; it lacked the sensitivity to define the number of days a window of opportunity exists. Additionally, it was limited to a single case study.

**Case Study 2: A Refined Window of Opportunity for Information Seeking**

The first case study found that media coverage of a previous event outside the window of opportunity did not significantly influence gun control support. This second case study posits that to influence change, information must fall within the three days following a crisis while people are actively and interactively seeking information. The second case study builds on the first case study by examining information-seeking behaviors based on Google Trends data that represents Google search intensity per day on a scale of 0-100. In addition to examining the duration of information-seeking, this case study examined three crises: the Boston Marathon bombing, the 2015 Paris attack, and Hurricane Matthew in 2016. Figure 1 reflects the information-seeking intensity resulting from Google searches, as reported by Google Trends.

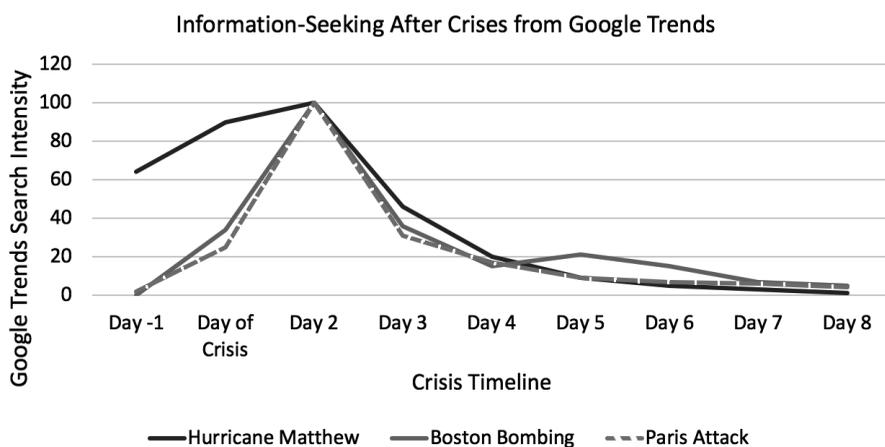


Figure 1. Crises Google Trends Data

The first two crises, the Boston bombing and the Paris attack, examine a similar type of crisis to see if there was any difference based on location. The third crisis, a hurricane, provided a different type of crisis to compare. The fourth crisis from the first case study provided another type of crisis to identify potential relationships. The information-seeking correlations between the crises were all significant.

Table 1. Correlations of Crises Google Trends Data

Variable	Hurricane Matthew	Boston Bombing	Paris Attack	Sandy Hook
<b>Hurricane Matthew</b>				
Pearson <i>r</i>	—	.69*	.70*	.71*
<i>P</i>	—	.039	.035	.033
<b>Boston Bombing</b>				
Pearson <i>r</i>	.70*	—	.99*	.93*
<i>P</i>	.039	—	.000	.000
<b>Paris Attack</b>				
Pearson <i>r</i>	.70*	.99*	—	.91*
<i>P</i>	.035	.000	—	.001
<b>Sandy Hook</b>				
Pearson <i>r</i>	.71*	.93*	.91*	—
<i>P</i>	.033	.000	.001	—

The result was a more refined period of information seeking from two weeks in the crisis opportunity model to three days, including the day of the crisis. When people are information-seeking, they have an increased susceptibility to information, including deception and disinformation<sup>[49]</sup> The day following the crisis would likely be most beneficial for message timing effectiveness. Whether the goal is to persuade or deceive a person, exposing the target population to the information during the first three days is essential. The sooner the exposure, the better as other information may fill the information void and terminate the need for orientation- and information-seeking behaviors. This research further refined the duration of active information-seeking behaviors identified in the first case study.

The information obtained in the information-seeking window of opportunity is then socialized. Information socialization is the second stage, and while influence can occur from the first window of opportunity, information is a social process that can produce longer term persuasive effects. Socialization of shared information increases its reach to passive information-seekers.

***Case Study 3: A Window of Opportunity for Information Socializing***

During the information socialization stage, information is shared with the person’s network for evaluation. Socializing information is an important step in people processing

uncertainty and accepting the information.<sup>[50]</sup> People seek information and bring it back to their social networks as a form of dyadic coping to aid in processing the information to understand the crisis and what it means.<sup>[51]</sup> People often socialize information as part of dyadic coping to confirm the information and news articles they consume.<sup>[52]</sup> Socialization can happen in discussions, social media, and community engagements and events. The timing of socialization peaks about three days after the event and then drastically reduces based on a study by Ney.<sup>[53]</sup> The study examined a Twitter data set for a couple of weeks following a tornado in Joplin, MO, using common keywords to the crisis. The estimated volume of tweets was the highest three days after the tornado, with nearly 220,000 tweets. Day four was second, with nearly 90,000 tweets. Day two was the third highest with about 50,000 tweets, then day five with 45,000 tweets. By day nine, tweets were at around 25,000 a day. This is an indicator of the duration of the window of information socialization.

**Relationship Between Case Studies**

The majority of information-seeking comes the day after the crisis, and the majority of socializing information occurs on the third day after the crisis. In the chart below, the similarities between each crisis are evident. Additionally, the Twitter volume was overlaid on the chart, with the volume ranging from 25,000 to 220,000 tweets a day.

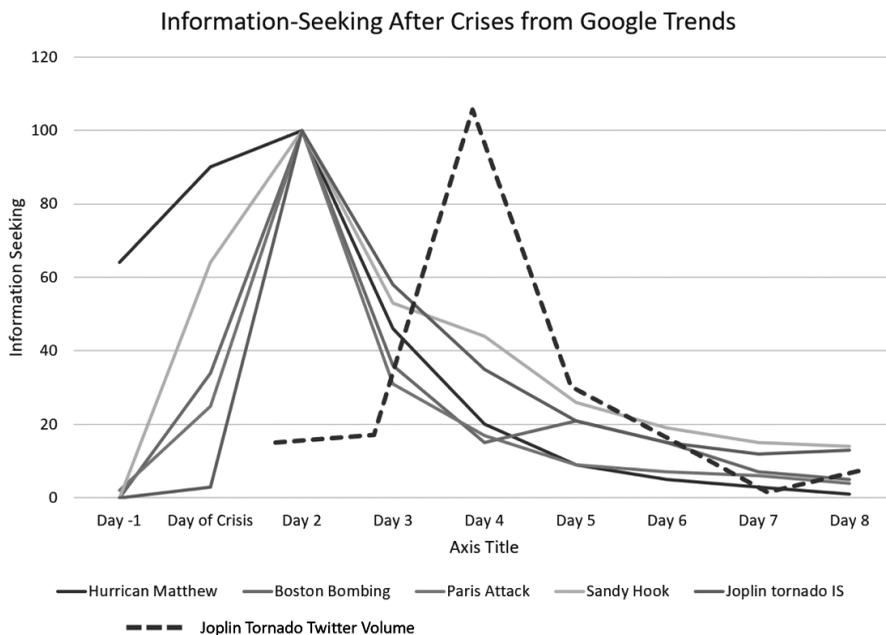


Figure 2. Crises Google Trends Data with Twitter Volume Overlaid

With one exception, the information-seeking between crises correlated with significant relationships ( $p < .05$ ,  $r = .693-.986$ ). A significant relationship was not found between the

tornado and hurricane. The tornado twitter volume correlated with the information-seeking ( $p < .01$ ,  $r = .880$ ). The twitter volume data was adjusted by two days to determine information seeking's influence on information-socialization. The influence of information-seeking on information socialization amplifies the significance of messaging during the initial window of opportunity. Examining the context of the socialized information can yield insights into the messaging's effectiveness during the information-seeking window of opportunity. Each case study amplifies the importance of timing, a limited opportunity due to the uncertainty caused by a focusing event.

### *Discussion*

The two stages of information-seeking and socialization mainly occur over five days. Event-based messaging associated with a narrative approach could demonstrate the effectiveness of the two windows of opportunity by initially determining that the message is received during the first window and then socialized, indicating the initial message was received and considered coherent. Subsequent messages designed explicitly for information-socialization offer opportunities to expand the reach to passive information seekers.

In a complex information environment, numerous groups or actors may attempt to fill the information void supporting a narrative. The importance of information processing should reflect in messaging approaches to increase messaging efficiency and effectiveness during the short windows of opportunity. During the information-seeking stage, messages about the focusing event provide meaning and open dialogue about the event and related issues. Furthermore, if measures of effectiveness are focused on each window, it can help determine if the message was received, accepted, socialized, and accepted by the social network. This provides a more nuanced understanding of the success of the messaging and influence effort.

### *Implications*

The research on information processing informs how to more effectively and efficiently message following significant events that spur information seeking and socialization. The windows are consistent between variations in focusing events. The implications of the windows relative to information processing span the range of influence activities from mass influence to precision, including deception efforts. To maximize messaging effectiveness during those windows, messaging and counter-messaging approaches must be developed well before the crisis or focusing event.

With an overarching narrative established, the planned delivery of the story must include numerous complementary messaging approaches to exploit broad and varied information channels, lines of persuasion, and types of messages. While some crises are not predictable, some have sufficient frequency to warrant deliberate planning in advance of a focusing event with products and messages drafted to ensure timely injection into the information environment during the appropriate windows. During the first window of opportunity, messaging

should focus on explaining the event within a historically consistent frame to support the desired narrative that connects the event to corresponding themes. As the information socialization window begins, messages to social groups through social networking sites and key communicators can accelerate socialization and increase acceptance. The distinct windows of opportunity should also guide message placement and design. The message, the medium, and the timing matter for each window of opportunity: the message development and design process should capture the nuances of each to ensure more deliberate, compelling messages.

### ***Limitations and Future Studies***

Future studies could further examine the similarities between crises and information-seeking and socialization. This study was limited and did not include social media data of the other four crises presented. A study that traces a single event through both windows of opportunities change in attitudes and support for an issue is warranted and would further amplify the implications.

### **CONCLUSION**

Information processing following a focusing event presents a unique opportunity to influence. Influence efforts should occur in a short window of time as there are only five days for information processing stages, seeking and socialization. The concept of timely messaging is not new. This research provides a more nuanced understanding of what timely means and establishes that the two windows of opportunity exist. The challenge to fill the information void during this time requires identifying the correct information channels and framing the information most favorable to given objectives that remain meaningful and relevant to the target audience. The inability to fill the information void leaves the interpretation of significant events to others, including those who seek to exploit crises to achieve nefarious or alternative goals.🛡️

NOTES

1. Dale E. Brashers and Timothy P. Hogan, "The Appraisal and Management of Uncertainty: Implications for Information-Retrieval Systems." *Information Processing & Management* 49, no. 6 (2013): 1241–49. <https://doi.org/10.1016/j.ipm.2013.06.002>.
2. Ibid.
3. Deanna D. Sellnow, *The Rhetorical Power of Popular Culture: Considering Mediated Texts*. Los Angeles, CA: SAGE, 2011.
4. Joshua S. McCarty, "Sandy Hook: A Case Study Approach Tracing the Crisis to Policy Support," 2017.
5. Walter R. Fisher, *Human Communication as Narration: toward a Philosophy of Reason, Value, and Action*. Columbia, SC: University of South Carolina Press, 1989.
6. Sellnow, *The Rhetorical Power of Popular Culture: Considering Mediated Texts*.
7. Ibid.
8. Thomas A. Birkland, "Focusing Events, Mobilization, and Agenda Setting," *Journal of Public Policy* 18, no. 1 (1998): 53–74. <https://doi.org/10.1017/s0143814x98000038>.
9. Matthew W. Seeger, Timothy L. Sellnow, and Robert R. Ulmer, *Communication and Organizational Crisis*, Westport, CT: Praeger, 2003.
10. Ibid, 5.
11. Timothy W. Coombs, *Ongoing Crisis Communication*, Thousand Oaks: SAGE Publications, 2015.
12. McCarty, "Sandy Hook: A Case Study Approach Tracing the Crisis to Policy Support."
13. Birkland, "Focusing Events, Mobilization, and Agenda Setting."
14. Ibid.
15. Michelle Wolfe, Bryan D. Jones, and Frank R. Baumgartner, "A Failure to Communicate: Agenda Setting in Media and Policy Studies." *Political Communication* 30, no. 2 (2013): 175–92. <https://doi.org/10.1080/10584609.2012.737419>.
16. Ibid.
17. A. Downs, "Up and down with Ecology: The Issue Attention Cycle." *Public Interest* 28 (n.d.): 28–50.
18. S. Hilgartner and C. Bosk, "The Rise and Fall of Social Problems: A Public Arenas Model." *American Journal of Sociology* 94 (1988): 53–78.
19. Birkland, "Focusing Events, Mobilization, and Agenda Setting."
20. Wolfe, Jones, and Baumgartner, "A Failure to Communicate: Agenda Setting in Media and Policy Studies," 175–92.
21. Ibid.
22. Joshua McCarty and Kaylee Laakso, "Understanding the Resource Curse with the Crisis Opportunity Model." *XIX International Sociology Association World Congress*. Toronto, 2018.
23. Birkland, Thomas A, "Focusing Events, Mobilization, and Agenda Setting," 53–74.
24. Eric Elmer Schattschneider and David Adamany, *The Semisovereign People: A Realist View of Democracy in America*. Fort Worth: Harcourt Brace Jovanovich college publ., 1975.
25. Ibid.
26. Birkland, "Focusing Events, Mobilization, and Agenda Setting," 53–74.
27. Ibid.
28. Brashers and Hogan, "The Appraisal and Management of Uncertainty: Implications for Information-Retrieval Systems," 1241–49.
29. Dale E. Brashers, Communication and Uncertainty Management. *Journal of Communication*, 51(3) (2001), 477-497. [doi:10.1111/j.1460-2466.2001.tb02892.x](https://doi.org/10.1111/j.1460-2466.2001.tb02892.x)
30. Timothy W. Coombs, *Ongoing Crisis Communication*, Thousand Oaks: SAGE Publications, 2015.
31. Brashers and Hogan, "The Appraisal and Management of Uncertainty: Implications for Information-Retrieval Systems," 1241–49.
32. Keri K. Stephens, Callish Malone, and Christine M. Bailey, "Communicating with Stakeholders During a Crisis: Evaluating Message Strategies," *The Journal of Business Communication* (1973) 42, no. 4 (October 2005): 390–419. [doi:10.1177/0021943605279057](https://doi.org/10.1177/0021943605279057).
33. C.K. Reissman, *Narrative Analysis*. Newbury Park, CA: Sage, 1993.

## NOTES

34. W.A. Afifi, Uncertainty and Information Management in Interpersonal Contexts, *New Directions in Interpersonal Communication Research*, 94-114. doi:10.4135/9781483349619.n5
35. L.K. Knobloch and K.G. Mcaninch, 13. Uncertainty management. *Interpersonal Communication*. doi:10.1515/9783110276794.297.
36. Ibid.
37. Ibid.
38. Brashers and Hogan, "The Appraisal and Management of Uncertainty: Implications for Information-Retrieval Systems," 1241-49.
39. T.L. Sellnow and M.W. Seeger, *Theorizing crisis communication*, 2013, Chichester, West Sussex: Wiley-Blackwell.
40. J. Kim and J. Lee, Knowledge Construction and Information Seeking in Collaborative Learning / La construction des connaissances et la recherche d'information dans l'apprentissage collaboratif, 2014, *Canadian Journal of Information and Library Science*, 38(1), 1-21. doi:10.1353/jils.2014.0005.
41. A. Carone and L. Di Iorio, "Crisis Management: An Extended Reference Framework for Decision Makers." *Journal of Business Continuity & Emergency Planning*, 6(4), 347-359.
42. Ibid.
43. K.R. Rossetto, Relational coping during deployment: Managing communication and connection in relationships, 2012, *Personal Relationships*, 20(3), 568-586. doi:10.1111/per.12000.
44. S. Moss, Subjective uncertainty reduction theory, 2009, <http://www.psych-it.com.au/psychlopedia/article.asp?id=252>.
45. P.L. Berger and T. Luckmann, *The social construction of reality: A treatise in the sociology of knowledge*, 2011, United States.
46. Sellnow, *The Rhetorical Power of Popular Culture: Considering Mediated Texts*.
47. McCarty, "Sandy Hook: a Case Study Approach Tracing the Crisis to Policy Support."
48. J. Uecker, *Religious and Spiritual Responses to 9/11*, Austin: National Institutes of Health, 2011.
49. Joshua McCarty and Kaylee Laakso, "Deception Opportunity Model," *International Conference on Deceptive Behavior*, Palo Alto, 2017.
50. Brashers and Hogan, "The Appraisal and Management of Uncertainty: Implications for Information-Retrieval Systems," 1241-49.
51. Ibid.
52. Carone and L. Di Iorio, "Crisis Management: An Extended Reference Framework for Decision Makers," 347-359.
53. Peter Ney, "Twitter and Natural Disasters," accessed March 15, 2020. <https://courses.cs.washington.edu/courses/cse544/13sp/final-projects/pl6-neyp.pdf>.





# The Global Engagement Center's Response to the Coronavirus Infodemic

---

Major Neill Perry

## INTRODUCTION

COVID-19 has underscored the shortcomings of the US government's (USG) approach to disinformation. Throughout the pandemic, adversary nations attacked both foreign perceptions of the US abroad as well as Americans' confidence in their own institutions. The US failed to execute a robust and coherent response against these spurious narratives. This article will review the federal government's actions with a particular focus on the Global Engagement Center (GEC), the agency nominally tasked to coordinate the federal government's response to foreign disinformation.

### *The US Retools After the Russian Influence Campaign*

The USG's current approach to disinformation evolved in response to recent foreign overtures. In 2016, the Russian government directed an influence campaign to sway the outcome of the US presidential election and to "undermine public faith in the US democratic process."<sup>[1]</sup> Under Kremlin direction, Russia's Internet Research Agency created online personas and inauthentic social media accounts to exacerbate a polarized American electorate. After the Russian interference campaign became public, the USG reorganized its fight against disinformation.

After the election in December 2016, Congress established the Global Engagement Center (GEC) "to lead, synchronize, and coordinate the USG's response to foreign state and non-state propaganda."<sup>[2]</sup> Congress further tasked GEC with coordinating with allies and partner nations, identifying which populations are the most susceptible to disinformation, analyzing current and emerging trends, and disseminating fact-based narratives to counter propaganda.<sup>[3]</sup> To foster interagency cooperation with the GEC, Congress authorized government agencies to detail their employees to the new agency.

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



**Major Neill Perry**, a U.S. Air Force Reserves intelligence officer assigned to the 446 Airlift Wing at Joint Base Lewis-McChord, Washington. As a civilian, he is a software engineer.

Congress organized this agency under the State Department because of the latter's traditional roles in official communication and foreign engagement.<sup>[4]</sup> In fact, the GEC is the latest iteration of a series of State Department agencies dedicated to countering foreign influence. The GEC itself replaced the Center for Strategic Counterterrorism Communications, which had replaced the Global Strategic Center, which replaced the Counterterrorism Communication Center.<sup>[5]</sup> However, these predecessor agencies focused on countering influence campaigns by violent extremist groups, such as ISIS. In the aftermath of the 2016 presidential election, GEC took on the much broader mission of leading the USG's fight against all disinformation.<sup>[6]</sup>

Despite the expansive congressional mandate, the GEC retreated towards a supporting role. "If I could really use one word to characterize the whole philosophical approach of the Global Engagement Center, it's partnerships,"<sup>[7]</sup> stated Daniel Kimmage, principal deputy coordinator at the GEC.<sup>[8]</sup> Mr. Kimmage explained that this approach is driven by the assumption that the USG is often "not the most effective communicator with most audiences." Instead, the agency focuses on identifying and supporting other organizations that are on the front line of disinformation. To support partner groups, the GEC distributes grants to local news agencies and civil society groups<sup>[9]</sup> and maintains an online platform—Disinfo Cloud—where groups can showcase their tools for fighting disinformation.<sup>[10]</sup>

The problem with the GEC's approach is that it is ill-suited for disinformation intended for American audiences. Instead, the GEC's approach seems to be a holdover from its predecessor agencies, which focused on countering ISIS propaganda.<sup>[11]</sup> The difference between the two types belies the GEC's principal assumption. To recruit new members, ISIS targeted Muslims, most of whom were not American.<sup>[12]</sup> From the perspective of a foreign audience, the USG was "not the most effective communicator."<sup>[13]</sup> Therefore, it made sense to let other entities and partners take the lead role against terrorist propaganda.

However, the GEC's assumption does not hold when the target audience is American. As the Senate Select Committee noted in its report, the operational focus of the 2016 Russian influence campaign was to "push Americans further away from one another, and foment distrust in government institutions."<sup>[14]</sup> The target audience for that influence campaign was the American people at large, not foreign nationals. And from the perspective of the domestic audience, the federal government would be a more effective communicator than civil groups. In this context, it is mistake for the GEC to remain quiet.

### *The COVID Infodemic*

The coronavirus ignited a global pandemic that has infected tens of millions and killed over one million people. It also sparked what the World Health Organization (WHO) labelled an "infodemic," a surfeit of lies and half-truths that undermine the public health response.<sup>[15]</sup> Like the COVID-19 virus, the infodemic has also infected millions of people and has cost lives.

COVID-19 has provided an ideal accelerant for disinformation. First, it is novel. Most people are unacquainted with the family of coronaviruses. Unlike maladies that have afflicted humanity for millennia, human coronaviruses were not identified until the 1960s.<sup>[16]</sup> Even experts have struggled to understand the new virus and its transmission vectors. From the outbreak, the public received conflicting and changing messages on the risks and the prophylactics of the virus. Second, the virus has inspired strong emotional reactions. It is lethal. As a new disease that threatens millions of people, it inspires anxiety.<sup>[17]</sup> News media showed images of patients on ventilators, overflowing hospitals, and numerous siren-blaring vehicles in lockdown cities. In sum, people fear the unknown and they fear death. These powerful emotional responses are a fertile environment for disinformation to flourish—and flourish it did.

The Empirical Studies of Conflict Project identified over 3,500 incidents of coronavirus-related disinformation.<sup>[18]</sup> There are hoaxes, scams, and fraudulent claims that coconut water, Clorox, breast milk, and vodka prevent or cure the disease. Many of these are perpetuated by charlatans and quacks; others are spread by leaders stoking ethnic or racial tension. Political leaders exploited the pandemic to continue their policies of blaming political opponents and ethnic minorities as a means of distracting from their own failures.<sup>[19]</sup>

Authoritarian governments also spewed disinformation. They did so in an effort to preserve their own power, curtail US and other Western influence, and erode confidence in democracy as a form of government.<sup>[20]</sup> Russia has engaged in disinformation campaigns targeting Western audiences to undermine trust in public health institutions.<sup>[21]</sup> Russia aims to "erode trust in institutions, such as host governments and traditional media, often by proliferating multiple false narratives."<sup>[22]</sup> Iran blames Israel and the US for creating the virus.<sup>[23]</sup> In a notable development, Chinese actors have begun to adopt Russian smear tactics, namely employing trolls and fake social media accounts to disseminate their message.<sup>[24]</sup> According to the GEC report, China, Russia, and Iran influence campaigns now echo one another.<sup>[25]</sup> Their common theme

is that the US shoulders responsibility for the pandemic because the disease originated as an American biological weapon.

### *GEC's Leadership of the Government Response*

GEC's actions during the pandemic have not measured up to the magnitude of the problem or the weight of GEC's responsibilities. For an entity responsible for coordinating USG's response to disinformation, the GEC has been strangely anonymous and has no social media presence. Without a Twitter or Facebook account, it relies on other government agencies to tweet out links to its reports.<sup>[26]</sup> The GEC's reticence stands in contrast to the Cybersecurity and Infrastructure Security Agency (CISA), which posts regularly to its Twitter, Facebook, LinkedIn, and YouTube accounts. CISA, a Department of Homeland Security component, aggressively used its social media accounts to counter disinformation during the 2020 presidential elections.

GEC has also been reluctant to share its expertise publicly. In February 2020, the Center identified a Russian disinformation campaign that involved thousands of social media accounts disseminating over two million tweets in multiple languages.<sup>[27]</sup> Allegedly, this campaign attributed the coronavirus to a diabolic ploy of American philanthropists, but GEC never released its report or otherwise shared its findings.<sup>[28]</sup> Silence in the fight against disinformation, is not a virtue. The global pandemic was an opportunity for the GEC to step up and warn the American people about ongoing foreign influence campaigns, but it failed to do so.

Other federal agencies have stepped in to counter the infodemic. The CISA created a COVID-19 Disinformation Toolkit to help state, local, and tribal governments combat disinformation.<sup>[29]</sup> The National Security Agency warned about foreign adversaries spreading disinformation online.<sup>[30]</sup> The Federal Bureau of Investigation (FBI) warned of coronavirus-related scams<sup>[31]</sup> and Chinese network intrusions against COVID-19 research organizations.<sup>[32]</sup> The Centers for Disease Control and Prevention (CDC) cautioned about coronavirus-related misinformation.<sup>[33]</sup> The Federal Emergency Management Agency (FEMA) established a Coronavirus Rumor Control website to provide authoritative information.<sup>[34]</sup> As other federal agencies reached out to the American people directly, the GEC seems to prefer to look inward towards its agency partners.

Experts who study disinformation recommend a bevy of solutions to stop disinformation, the most relevant to this article is the need for a whole of government approach.<sup>[35]</sup> This approach accepts the reality that no single agency can do it alone: "No single department or agency possesses the clout, expertise, or resources to make things happen across the USG on the scale needed to counter Russian disinformation."<sup>[36]</sup> Each federal agency has its own unique tools. For instance, Department of Defense (DoD) can disrupt botnet armies that disseminate misinformation, which is what U.S. Cyber Command (USCYBERCOM) did during the 2020 election season.<sup>[37]</sup> The Department of Justice (DOJ) is empowered to prosecute those who spread disinformation on behalf of foreign governments under the Foreign Agent Registration Act, which it did against the Internet Research Agency for its role in the 2016 elections.<sup>[38]</sup>

### *Déjà Vu All Over Again*

In 2019, just as the coronavirus pandemic was beginning, Congress created another center dedicated to fighting disinformation.<sup>[39]</sup> This time, Congress directed the Office of the Director of National Intelligence (ODNI) to create a Foreign Malign Influence Response Center (FMIRC). This new center will “serve as the primary organization in the United States Government for analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to foreign malign influence.”<sup>[40]</sup> The FMIRC will also provide assessments and reports about foreign malign influence to Congress and federal agencies,<sup>[41]</sup> and the director of the FMIRC may recommend “potential responses by the United States to foreign malign influence.”<sup>[42]</sup>

The decision to create a new agency is puzzling for two reasons. First, the FMIRC duplicates the mission of the GEC. The GEC already produces assessments on influence operations, including a team of thirty data scientists who monitor the public information environment and share their analysis with the State Department and interagency partners.<sup>[43]</sup> Second, Congress did not elaborate on how the FMIRC would work with the GEC. In passing this legislation, Congress did not eliminate the GEC or reduce its mission. Not only does the GEC continue to exist, it may soon wield greater resources. In May 2021, the Senate passed legislation that would double the GEC’s annual budget<sup>[44]</sup> and would encourage the GEC to exchange liaison officers with the National Counterterrorism Center, the combatant commands, and other federal agencies.<sup>[45]</sup>

At this point, any discussion of how the two agencies will cooperate is academic. Congress passed the enabling legislation in 2019, but at the time of this article’s publication, the FMIRC does not yet exist. The Trump administration did not create the agency during the last year of its term,<sup>[46]</sup> and the Biden administration still has not done so. In April 2021, the new Director of National Intelligence, Avril Haines, testified she was “moving with alacrity towards” establishing the FMIRC. Director Haines indicated that she wanted the FMIRC to avoid duplicating existing efforts within the USG.<sup>[47]</sup>

Nations and private actors exploited the coronavirus pandemic to publish disinformation to support their preexisting agendas.<sup>[48]</sup> Authoritarian regimes sought to undermine US world standing and to erode Americans’ confidence in their government. The USG mounted a scatter-shot response against these narratives even as some federal agencies used their social media accounts and websites to warn about the presence of disinformation and redirect citizens to trustworthy sources. Although tasked with coordinating the USG’s response to disinformation, the GEC remained in the background. The GEC’s recent performance reifies one critique that the GEC “essentially operates as a grant-making body.”<sup>[49]</sup> Congress and the Biden administration should reform both the GEC and the federal government’s response as a whole. Although the pandemic will eventually subside, disinformation will endure.🛡️

**NOTES**

1. U.S. Senate Select Committee on Intelligence, Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of Social Media with Additional Views, [https://www.intelligence.senate.gov/sites/default/files/documents/Report\\_Volume2.pdf](https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf).
2. U.S. Congress, National Defense Authorization Act for Fiscal Year 2017, <https://www.congress.gov/bill/114th-congress/senate-bill/2943/text>.
3. U.S. Congress, National Defense Authorization Act for Fiscal Year 2017, <https://www.congress.gov/bill/114th-congress/senate-bill/2943/text>.
4. Lumpkin, M., "Countering Adversarial Propaganda Hearing for Members of the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, October 22, 2015, <https://docs.house.gov/meetings/AS/AS26/20151022/104086/HHRG-114-AS26-Wstate-LumpkinM-20151022.pdf>.
5. Office of the Spokesperson, U.S. State Department, "The Global Engagement Center" (July 6, 2016), <https://2009-2017.state.gov/r/pa/prs/ps/2016/07/259376.htm>.
6. LaGraffe, M., "Global Engagement: Center Seeks to Counter Terror Groups," *State Magazine* (Issue 616) October 2016.
7. Vincent, B., "How State's Disinformation-Fighting Arm Uses Artificial Intelligence," *Nextgov* (April 16, 2021), <https://www.nextgov.com/emerging-tech/2021/04/how-states-disinformation-fighting-arm-uses-artificial-intelligence/173401>.
8. Daniel Kimmage's LinkedIn page, accessed August 28, 2021, <https://www.linkedin.com/in/danielkimmage>.
9. Taylor, G., "State Department Global Engagement Center Targets Russian Propaganda, 'Deep Fakes,'" *The Washington Times* (December 12, 2018), <https://apnews.com/article/9f7892a163582b5fd0297e2a81124c35>.
10. U.S. State Department, "Disinfo Cloud," <https://www.state.gov/disinfo-cloud-launch/>.
11. Daniel Kimmage, "Policy Forum: Countering and Exposing Terrorist Propaganda and Disinformation," (February 17, 2021), <https://www.youtube.com/watch?v=HTUHW9ldyZ>.
12. Koerner, B.I., "Why ISIS Is Winning the Social Media War," *Wired* (March 2016), <https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat>.
13. Katz, R., "The State Department's Twitter War with ISIS Is Embarrassing," *Time* (September 14, 2014), <https://time.com/3387065/isis-twitter-war-state-department>.
14. Senate Intelligence Committee, Report on Russian Active Measures Campaigns, Volume 2.
15. World Health Organization, "Managing the COVID-19 Infodemic: Promoting Healthy Behaviors and Mitigating the Harm from Misinformation and Disinformation" (September 23, 2020), <https://www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation>.
16. Centers for Disease Control and Prevention, "Human Coronavirus Types" (February 15, 2020), <https://www.cdc.gov/coronavirus/types.html>.
17. P. Beaumont, et al., "Malicious Forces Creating 'Perfect Storm' of Coronavirus Information," *The Guardian* (April 24, 2020), <https://www.theguardian.com/world/2020/apr/24/coronavirus-sparks-perfect-storm-of-state-led-disinformation>.
18. J. Shapiro, et al., "ESOC COVID-19 Disinformation Tracking Report," (2020), <https://esoc.princeton.edu/publications/esoc-covid-19-disinformation-tracking-report>.
19. T. Erdemir, et al., "Usual Suspects: Iran and Turkey's Scapegoating of Minorities During Covid-19," *Anti-Defamation League* (June 11, 2020), <https://www.adl.org/blog/usual-suspects-iran-and-turkeys-scapegoating-of-minorities-during-covid-19>.
20. K. Stricklin, "Why Does Russia Use Disinformation?," *Lawfare* (March 29, 2020), <https://www.lawfareblog.com/why-does-russia-use-disinformation>.
21. G. Corn, "Coronavirus Disinformation and the Need for States to Shore Up International Law" (April 2, 2020). <https://www.lawfareblog.com/coronavirus-disinformation-and-need-states-shore-international-law>.
22. T. Helmus, et al., "Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe," *Rand Corporation*, 2018, [https://www.rand.org/content/dam/rand/pubs/research\\_reports/RR2200/RR2237/RAND\\_RR2237.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf).
23. K. Aarabi, "Iran Knows Who to Blame for the Virus: America and Israel," *Foreign Policy* (March 19, 2020), <https://foreign-policy.com/2020/03/19/iran-irgc-coronavirus-propaganda-blames-america-israel/>
24. J. Kurlantzick, "How China Ramped Up Disinformation Efforts During the Pandemic," *Council on Foreign Relations*, September 10, 2020, <https://www.cfr.org/in-brief/how-china-ramped-disinformation-efforts-during-pandemic>.

## NOTES

25. B. Swan, "State Report: Russian, Chinese and Iranian Disinformation Narratives Echo One Another," Politico (April 21, 2020), <https://www.politico.com/news/2020/04/21/russia-china-iran-disinformation-coronavirus-state-department-193107>.
26. National Counterintelligence and Security Center (August 5, 2020), <https://twitter.com/NCSCgov/status/1291146503499767809>.
27. L. Kelly, "US Paints Murky Picture of Russian Disinformation on Coronavirus," *The Hill* (March 12, 2020), <https://thehill.com/policy/international/487150-us-paints-murky-picture-of-russian-disinformation-on-coronavirus>.
28. Swan, "State Report: Russian, Chinese and Iranian Disinformation Narratives Echo One Another."
29. Cybersecurity and Infrastructure Security Agency, "Coronavirus," <https://www.cisa.gov/coronavirus>.
30. National Security Agency (October 9, 2020), <https://twitter.com/NSAGov/status/1314656984084418560>.
31. Federal Bureau of Investigation, "Federal Agencies Warn of Emerging Fraud Schemes Related to COVID-19 Vaccines," (December 21, 2020), <https://www.fbi.gov/news/pressrel/press-releases/federal-agencies-warn-of-emerging-fraud-schemes-related-to-covid-19-vaccines>.
32. Federal Bureau of Investigation, "FBI and CISA Warn Against Chinese Targeting of COVID-19 Research Organizations," (May 13, 2020), <https://www.fbi.gov/news/pressrel/press-releases/fbi-and-cisa-warn-against-chinese-targeting-of-covid-19-research-organizations>.
33. Centers for Disease Control and Prevention (March 23, 2020), <https://twitter.com/CDCgov/status/124211586114163201>.
34. Federal Emergency Management Agency, Coronavirus Rumor Control, last updated August 25, 2020, <https://www.fema.gov/disasters/coronavirus/rumor-control>.
35. A. Polyakova, et al., "Democratic Defense Against Disinformation 2.0," Atlantic Council Eurasia Center (June 2019), [https://www.atlanticcouncil.org/wp-content/uploads/2019/06/Democratic\\_Defense\\_Against\\_Disinformation\\_2.0.pdf](https://www.atlanticcouncil.org/wp-content/uploads/2019/06/Democratic_Defense_Against_Disinformation_2.0.pdf).
36. J. Farwell, "Countering Russian Meddling in US Political Processes," *Parameters* (Spring 2018): 39.
37. E. Nakashima, "Cyber Command Has Sought to Disrupt the World's Largest Botnet, Hoping to Reduce Its Potential Impact on the Election," *The Washington Post* (October 9, 2020), [https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-af66-dc429b380d10\\_story.html](https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-af66-dc429b380d10_story.html).
38. U.S. Department of Justice, "Recent FARA Cases," (February 26, 2021), <https://www.justice.gov/nsd-fara/recent-cases>.
39. 116<sup>th</sup> Congress, S. 1790 §5322, National Defense Authorization Act for Fiscal Year 2020, <https://www.congress.gov/bill/116th-congress/senate-bill/1790>.
40. 50 U.S.C §3059(b)(3).
41. 50 U.S.C §3059(b)(4).
42. 50 U.S.C §3059(c)(2)(C).
43. Daniel Kimmage, "Policy Forum: Countering and Exposing Terrorist Propaganda and Disinformation," Washington Institute (February 17, 2021), <https://www.youtube.com/watch?v=HTUHW9ldyZ>.
44. Office of U.S. Senator Rob Portman, "Press Release: Portman, Murphy Applaud Inclusion of Provision to Fight Global Propaganda and Disinformation in Senate Passage of U.S. Innovation and Competition Act" (June 8, 2021), <https://www.portman.senate.gov/newsroom/press-releases/portman-murphy-applaud-inclusion-provision-fight-global-propaganda-and>.
45. 117<sup>th</sup> Congress, S.1260 § 3137(c), United States Innovation and Competition Act of 2021, <https://www.congress.gov/bill/117th-congress/senate-bill/1260/text>.
46. Office of U.S. Senator Amy Klobuchar, "Press Release: Klobuchar, Reed, Peters Urge National Security Officials to Take Steps to Counter Foreign Influence Campaigns," (February 25, 2021), <https://www.klobuchar.senate.gov/public/index.cfm/news-releases?ID=IEDA4FBA-8E2B-4ADD-8AFA-5D762856B20B>.
47. *Worldwide Threats: Testimony before the Committee on Armed Services*, 117<sup>th</sup> Congr., (2021)(testimony of Avril Haines, Director of National Intelligence).
48. U.S. State Department, *GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem* (August 2020), <https://www.state.gov/russias-pillars-of-disinformation-and-propaganda-report>.
49. N. Jankowicz, *How to Lose the Information War* (London: I.B. Tauris, 2020), 196.



# THE CYBER DEFENSE REVIEW

◆ BOOK REVIEW ◆



*Bitskrieg: The New Challenge of Cyberwarfare*

By John Arquilla

Reviewed by  
Major Mathieu Couillard



**EXECUTIVE SUMMARY**

In the 1990s, John Arquilla and David Ronfeldt co-authored an influential series of articles in which they developed the concepts of cyberwar, swarming tactics, and netwar. Drawing on historical analogies that predate the information age, he articulated how information dominance would critically enable future warfare. Today, some senior leaders herald this concept as the centerpiece to strategic success. In *Bitskrieg*, the professor emeritus at the U.S. Naval Postgraduate School once again draws from history to envision the evolution of conflict. He possesses rich experience to complement it, as he has had fortune to witness and influence US strategic decision-making for the last three decades. In his book, Arquilla provides strategic context for ongoing efforts to increase the use of cloud computing and strong encryption, and articulates a new approach to cyber arms control agreements. His work is insightful to practitioners and leaders throughout the cyber domain.

**REVIEW**

The memorable title of the book is an obvious reference to the devastating armored breakthrough tactics employed by Germany at the onset of World War II—and, more optimistically, to the allies' ability to defeat this strategy over time. Arquilla laments that the United States has thus far failed to adapt to the cyber threat, allowing freedom



**Major Mathieu Couillard** is a Signals Officer in the Canadian Armed Forces. He has served with conventional and special operations forces in network and cyber operations leadership roles. Major Couillard holds a bachelor's degree in computer engineering and is currently a student at the U.S. Naval Postgraduate School in the Defense Analysis Department. His research will focus on the role of deception in cyber strategy.

of action in cyberspace to rival powers such as China and Russia, and even to lesser nations such as North Korea—described as a “strategic criminal.” Bitskrieg goes beyond the cyber domain; it is an appeal for a paradigm shift from a centralized “few large” approach (i.e., Blitzkrieg) to a decentralized “many small” swarm, which heavily relies on information dominance. Arquilla suggests this can be achieved through technological, doctrinal, and organizational reform. He smoothly transitions between relevant historical analogies and firsthand accounts, notably of the Gulf War, to illustrate this concept.

Building on the title's World War II analogy, Arquilla compares traditional perimeter-based cyber defense to the catastrophically ineffective Maginot Line. Arquilla invites the reader to “imagine no lines,” and assume the inevitable breach of perimeter defenses. He recommends the employment of strong encryption in depth, which is well underway with the ubiquity of Hypertext Transfer Protocol Secure (HTTPS) and rapid adoption of Zero Trust. He also promotes use of the cloud and data mobility, stating that “data at rest are data at risk.” This is valid for the majority of organizations (including within the military), which benefit from the enhanced availability, data center security, monitoring, and up-to-date baselines that the cloud provides. However, there are attack strategies that specifically target data in transit, and cloud providers are not immune to breaches or subversion. Hence, one must carefully weigh the risks and benefits of the cloud relative to closed, on-premises networks for their most valuable data. Nonetheless, decision-makers must urgently adopt Arquilla's overall recommendation to evolve from perimeter defense to defense-in-depth.

In addition to deepening defenses, Arquilla argues that cyber arms control agreements could lead to greater stability in the cyber domain. He recognizes that most observers assume these efforts to be futile; the attribution problem in cyberspace and the “dual use” of information technology (i.e., the challenge in distinguishing offensive and defensive cyber capabilities) have long hindered such treaties. Instead of “structured arms control,” where cyber weapons would be inventoried like nuclear warheads, Arquilla suggests a behavioral approach. In this logic, agreements would focus on limiting attacks against certain targets (e.g., civilian infrastructure) rather than banning a certain type or quantity of cyber weapons. In a fascinating passage, many will be surprised to discover that Russia once proposed such agreements to the US. Indeed, Arquilla led a delegation to a summit where top Russian cyber officials made just such an overture which was promptly rejected by US decision-makers. These leaders presumably assumed that cyber superiority would guarantee protection, just as previous superiority in other domains; unfortunately, this assumption has resoundingly been proven wrong. Today, Russia is a declining power by nearly all metrics but continues to project power effectively through cyber attacks and information warfare. As all societies are increasingly dependent on the Internet and leaders become aware of its incongruent reflection of power, a solution must be found to better manage cyber conflict. One can only hope that Arquilla’s recommendations will lead down a fruitful path.

## CONCLUSION

Ultimately, *Bitskrieg* is a quick and enlightening read that will satisfy both technically and policy-focused readers. Arquilla convincingly not only predicts how warfare will be waged but also how to defend against it. The pervasiveness of cloud deployments and strong encryption is empirical evidence that supports Arquilla's thesis but also suggests they may not be useful to practitioners who have already arrived at the same conclusion. However, there is still much progress to be made in these areas, and Arquilla’s narrative can help the technical community explain the imperatives in strategic terms that can be understood by policymakers. ♥

Title: *Bitskrieg: The New Challenge of Cyberwarfare*

Publisher: Polity

Paperback: 240 pages

Language: English

ISBN-13: 978-1-509-54363-2

EISBN: 978-1-509-54364-9

Price: \$22.95 (Paperback)

Price: \$64.95 (Hardcover)

Price: \$14.00 Kindle edition

## NOTES

1. John Arquilla and David Ronfeldt, "Cyberwar Is Coming!" in *In Athena's Camp: Preparing for Conflict in the Information Age* (RAND Corporation, 1992), <https://www.rand.org/pubs/reprints/RP223.html>; John Arquilla and David Ronfeldt, "The Advent Of Netwar" (RAND Corporation, January 1, 1996), [https://www.rand.org/pubs/monograph\\_reports/MR789.html](https://www.rand.org/pubs/monograph_reports/MR789.html); and John Arquilla and David Ronfeldt, "Swarming and the Future of Conflict" (RAND Corporation, January 1, 2000), [https://www.rand.org/pubs/documented\\_briefings/DB311.html](https://www.rand.org/pubs/documented_briefings/DB311.html).
2. John Arquilla, "The Strategic Implications of Information Dominance," *Strategic Review* 22 (1994): 22-34.
3. Riad Kahwaji, "'The Future Is About Information Dominance': Gen. Nakasone," *Breaking Defense* (blog), June 29, 2021, <https://breakingdefense.sites.breakingmedia.com/2021/06/the-future-is-about-information-dominance-gen-nakasone/>.
4. John Arquilla, *Bitskrieg: The New Challenge of Cyberwarfare*, 1st edition (Polity, 2021), xix.
5. Arquilla, xvi.
6. Arquilla, 79.
7. Arquilla served as a member of an advisory team to U.S. Army General Norman Schwarzkopf from August 1990 to February 1991. See Arquilla, 15.
8. Arquilla, 43.
9. According to a report from Microsoft Security, Zero Trust is critical to 96 percent of security decision-makers, with 76 percent of organizations having at least started its implementation. However, only 35 percent of the organizations polled have completed their implementation. See Microsoft Security, "Zero Trust Adoption Report," July 2021, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWGWha>.
10. Arquilla, *Bitskrieg*, 45.
11. Bruce Schneier and Herr Trey, "Russia's Hacking Success Shows How Vulnerable the Cloud Is," *Foreign Policy* (blog), accessed October 26, 2021, <https://foreignpolicy.com/2021/05/24/cybersecurity-cyberattack-russia-hackers-cloud-sunburst-microsoft-office-365-data-leak/>.
12. For example, the US and China signed an agreement in 2015 but routinely accuse each other of violations, which the other party denies by leveraging the ambiguity of the cyber domain. See Emily Feng, "The White House Blamed China for Hacking Microsoft. China Is Pointing Fingers Back," *NPR*, July 20, 2021, sec. National Security, <https://www.npr.org/2021/07/20/1018283149/china-blames-united-states-for-cyberattacks>.
13. Arquilla, *Bitskrieg*, 110.
14. Arquilla, 105-6.
15. The Solar Winds Attack is the most recent example of Russian might in cyberspace. See David E. Sanger, Nicole Perloth, and Julian E. Barnes, "As Understanding of Russian Hacking Grows, So Does Alarm," *The New York Times*, January 2, 2021, sec. U.S., <https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html>.







# THE CYBER DEFENSE REVIEW

CONTINUE THE CONVERSATION ONLINE

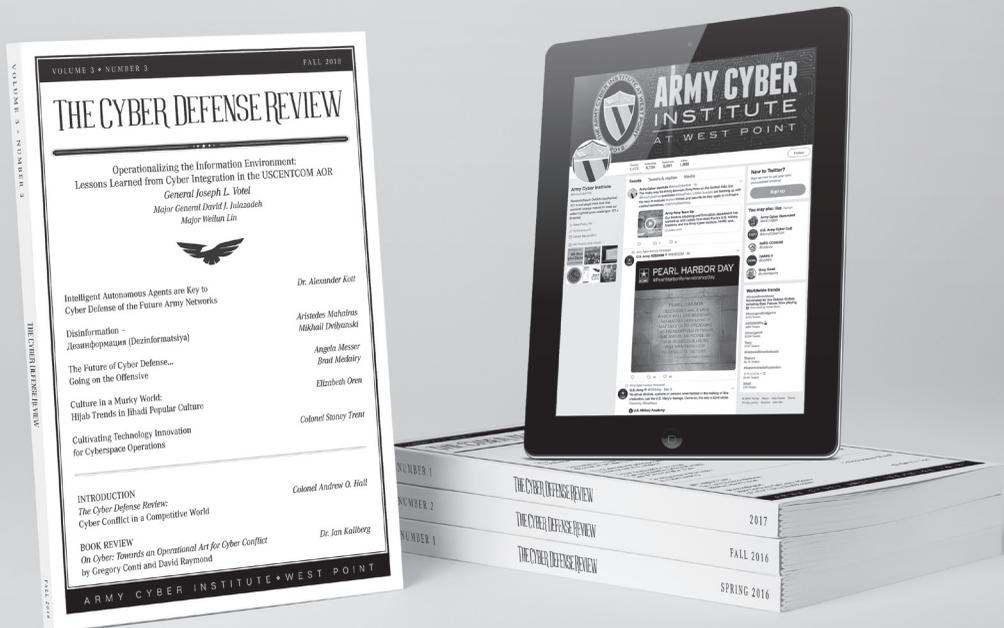
 [CyberDefenseReview.Army.mil](http://CyberDefenseReview.Army.mil)

AND THROUGH SOCIAL MEDIA

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

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

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



ARMY CYBER INSTITUTE ♦ WEST POINT





---

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