The Information Domain: An Argument for Organization

A Monograph

by

Mr. Brian F. Burke
US Department of Defense

School of Advanced Military Studies
US Army Command and General Staff College
Fort Leavenworth, KS

2021

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
23 05 2019	MASTER'S MONOGRAPH	JUNE 18-MAY 19

4. TITLE AND SUBTITLE
The Information Domain: An Argument for Organization

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Brian F. Burke

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
ADVANCED MILITARY STUDIES PROGRAM

10. SPONSOR/MONITOR'S ACRONYM(S)
SAMS AMSP

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Current bureaucratic "stove piping" and committee-based interagency interactions are inadequate for defending the Information Domain and achieving stated policy directives. A more agile, holistic, and integrated effort is required, including changes to operating organizations and legal authorities to achieve the desired protection while retaining essential liberties. Freedom of speech is vital for individual liberty, the security of which is the reason for government in the United States. The US, and the West in general, are different from autocratic competitors in this effort to preserve and protect individual liberty. Freedom of speech and association, both hallmarks of the internet and the global communications it has enabled, are American ideas. Every individual has a right to present their ideas to other people. This presentation of ideas is the bedrock of all social interaction. The US Government is only allowed to abridge free speech or freedom of expression under very specific circumstances. The DoD risks such abridgment by taking on information warfare as part of its cyberspace mission by curating online content, whether directly or by proxy. Stretching of new permissions under new DoD authorities meant to allow freedom of action and proportional response may make DoD wittingly or unwittingly a censor of Americans. Such action without clear authorities create potential political and legal liabilities for DoD and undermines US Government credibility as its actions in the domain mirror the adversary autocracies with which the US competes.

15. SUBJECT TERMS
Information, Cyberspace, Homeland Security, Law, Doctrine, Security, Government

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	59	913 758-3300

Monograph Approval Page

Name of Candidate: Mr. Brian F. Burke

Monograph Title: Organizing for Information Domain

Approved by:

__//signed/27 MAR 21/MSM//_____, Monograph Director
Matthew S. Muehlbauer, PhD

__//signed/29 MAR 21/JMA//_____, Seminar Leader
Jason M. Alvis, COL

//signed 23 APR 21/ BAP, Director, School of Advanced Military Studies
Brian A. Payne, COL

Accepted this 20th day of May 2021 by:

_____, Assistant Dean of Academics for Degree Programs and Research
Dale F. Spurlin, PhD

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the US Army Command and General Staff College or any other government agency. (References to this study should include the foregoing statement.)

Abstract

Organizing for Information Domain, by Mr. Brian F. Burke, 65 pages.

Current bureaucratic “stove piping” and committee-based interagency interactions are inadequate for defending the Information Domain and achieving stated policy directives. A more agile, holistic, and integrated effort is required, including changes to operating organizations and legal authorities to achieve the desired protection while retaining essential liberties. Freedom of speech is vital for individual liberty, the security of which is the reason for government in the United States. The US, and the West in general, are different from autocratic competitors in this effort to preserve and protect individual liberty. Freedom of speech and association, both hallmarks of the internet and the global communications it has enabled, are American ideas. Every individual has a right to present their ideas to other people. This presentation of ideas is the bedrock of all social interaction. The US Government is only allowed to abridge free speech or freedom of expression under very specific circumstances. The DoD risks such abridgment by taking on information warfare as part of its cyberspace mission by curating online content, whether directly or by proxy. Stretching of new permissions under new DoD authorities meant to allow freedom of action and proportional response may make DoD wittingly or unwittingly a censor of Americans. Such action without clear authorities create potential political and legal liabilities for DoD and undermines US Government credibility as its actions in the domain mirror the adversary autocracies with which the US competes.

Contents

Acknowledgments

To my wife and children, you are the reason I aspire to do these things, always, thank you. For my friends and colleagues in Cyberia, see this is what happens when I am allowed to think and write with adult supervision. My gratitude to my syndicate lead, Dr. Matthew Muehlbauer, whose advice, patience, and mentorship made this monograph possible. To COL Jason Alvis, USA, whose leadership inspired the rest of the B-Team and me, I also say thanks, hooah. To the members of Seminar 2 AMSP 2021, the B-Team, thank you for your humor, encouragement, camaraderie, and the creation and hosting of Think and Drink sessions, which helped shape my understanding as my research and writing matured. A shout out to all the staff at the Ike Skelton Combined Arms Research Library for all your assistance in finding sources and enabling this digital immigrant to gain library skills beyond the card catalog. Finally, thanks to God for setting me on this path to meet and learn from you all. Peace.

Abbreviations

ARPANET	Advanced Research Projects Agency Network
BRICS	Brazil, Russia, India, China, and South Africa
C2	Command and Control
CCDCOE	Cooperative Cyber Defense Center of Excellence
CISA	Cybersecurity and Infrastructure Security Agency
CSC	Cyberspace Solarium Commission
DHS	Department of Homeland Security
DoD	Department of Defense
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FSB	Federal Security Service
NDAA	National Defense Authorization Act
NSA	National Security Agency
SEC	Securities and Exchange Commission
SORM	System for Operative Investigative Activities
UN	United Nations
USCYBERCOM	United States Cyber Command

Illustrations

Introduction: The Information Domain

> So, the National Security Agency is a foreign intelligence organization, it is not a domestic intelligence organization. There are specific legal constraints placed on us when it comes to collection against US persons. US persons includes the definition of a US entity in the form of a company. We're specifically legally limited from doing that. We do not have a presence on US private networks inside companies. That's not what we're about, that's not what our mission is. It's because of that lack of awareness, if you will, on our part that I'm saying, look, I need a partnership here. We need to exchange information.
>
> —Director NSA/Commander USCYBERCOM Admiral Rodgers,
> *Hearing of the House (Select) Intelligence Committee Nov 2014*

In December 2020, news broke of a widespread computer hack of US Government systems, likely by Russian state cyber actors, via software produced by the company Solarwinds. The software provides a suite of tools for remote access and network management for its customers, primarily companies needing remote management capabilities for their online presence. According to December media reports, the Russian hack of Solarwinds provided access to up to 18,000 customers.[1] However, the depth of the compromise may never be known, as a forensic examination of the hack found that the Russian actors had access to Solarwinds customers as early as March 2020 and were not discovered until December.[2] The victims and the US Government may never know how compromised these systems are because administrative levels of access acquired by the hackers enable complete control and manipulation and the ability to destroy any evidence.

The first government report concerning this hack was from the Securities and Exchange Commission (SEC) in a December 14, 2020 filing form 8-K. This form is used to report any

[1] Isabella Jibilian, "Here's a Simple Explanation of How the Massive SolarWinds Hack Happened and Why It's Such a Big Deal," *Business Insider*, December 24, 2020, accessed December 25, 2020, https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.

[2] FireEye, "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor," *FireEye* (blog), December 13, 2020, accessed December 13, 2020, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html.

unscheduled material events, in this case, a cyber-attack, or corporate changes at a company that could be of importance to the shareholders or the SEC. The final line in that report is an indicator of the government defense problem in the Information Domain. "All information provided in this Current Report on Form 8-K is as of the date hereof, and SolarWinds undertakes no duty to update this information except as required by law."[3] Though the government seeks partnerships with the private sector, commercial companies will only report when compelled by law or cooperation is in their bottom line's best interest.

Legal constraints on US military, intelligence, regulatory agencies, and law enforcement entities limit their actions and results in a lack of coherent presence and situational awareness concerning the US portions of the Information Domain. These are similar to the US Intelligence Community's structure before the terror attacks on 9/11 and eerily akin to the intelligence failures which led to the weapons of mass destruction assessments underpinning the 2003 US invasion of Iraq. There is a "siloed" enforcement structure stifling monitoring, inter-agency communications, and creating failures in warning and delays in response. Lack of information sharing and among entities focused on warning in the Information Domain, as evidenced by the Solarwinds hack, creates a national security concern. Moreover, government organizations with the capability to regulate, enforce the law, and operate in the Information Domain were all legally established accomplish missions other than regulating the domain itself. Instead, the US Government seeks to repurpose or stretch mission definitions or use a foreign intelligence collection or criminal law enforcement entities to "protect" from cyber-attack.

The legal constraints on using capabilities to conduct general surveillance or monitoring of the Information Domain are linked to the constitutional freedom of speech and protection from unreasonable search and seizure. Prior abuses of these capabilities have resulted in government-

[3] Kevin Thompson, "Statement of Changes in Beneficial Ownership," *United States Securities and Exchange Commission, File Number 001-38711*, December 14, 2020, accessed December 14, 2020, https://www.sec.gov.

wide programs for intelligence oversight and, for some people, created or reinforced a general distrust of the government organizations possessing such capabilities. Elements within the Information Domain already retell this narrative. One only has to look at popular entertainment, which casts intelligence agencies as dark entities that use innocent people as pawns in more significant games.[4] However, the threats are real, and legal constraints create ethical dilemmas for those entities possessing capability.

These dilemmas and the associated mismatch of authorities and organization is not new. As far back as 2010, the *New York Times* quoted General Keith Alexander, who said there was a "mismatch between our technical capabilities to conduct operations and the governing laws and policies."[5] In the years since, cyberspace has matured with emergent properties creating both opportunities and threats. Those threats and the continued related mismatches in capability are related mainly to globalization and the adoption of information technologies to share ideas. In light of this emergence and demonstrated inadequacies of current structures, it is time to ask how the United States should adequately organize to defend itself from information threats.

To consider way forward, this paper will examine how the US does and has viewed the Information Domain and how the chief competitors of the US view the Information Domain and use it. Such a review, coupled with analysis and consideration of the US "defense" view of the domain and current government organizational constructs, will frame understanding and will generate potential alternatives for the US Government to consider. These will possibly offer new or different organizational constructs and legal authorities enabling cohesive action in the domain including but not limited to regulation, monitoring, defense, and integration of national efforts to secure the peoples' liberty.

---

[4] *Blackhat*, directed by Michael Mann, Internet Movie Database, January 14, 2015, accessed 20 December 2020, https://www.imdb.com/title/tt2717822/?ref_=fn_al_tt_1.

[5] Thom Shanker, "Cyberwar Nominee Sees Gaps in Law," *The New York Times*, April 14, 2010, accessed 20 December 2020, https://www.nytimes.com/2010/04/15/world/15military.html.

The US Government is not organized to effectively protect itself and its citizens from threats emanating from the Information Domain. This vulnerability is because the US, unlike its competitors, continues to treat the information environment and cyberspace as separate entities that are addressed by disparate regulatory frameworks, rather than as a holistic arena with its own requirements for regulation and defense. The government has made a substantial effort to address cybersecurity issues, as evidenced in the creation of United States Cyber Command (USCYBERCOM) and the Cyber Infrastructure Security Agency. These efforts, however, are primarily linked to actions protecting government and military networks and communicating best practices to businesses and citizens about defending themselves. They fail to give adequate attention to the "commons" as integral part of the operating environment is the Information Domain, and the need to protect it.[6] A look at foreign actors' actions to safeguard their Information Domain and their national sovereignty indicates a potential need for changes to legal, regulatory, and possible organizational changes to improve the US approach.

The US need for such changes becomes more apparent when comparing its military doctrinal view of the Information Domain against that of the other physical domains. The US has specific military, homeland defense, regulatory bodies, and law enforcement agencies, each with specific legal authority to act in physical domains. To protect an emergent Information Domain, the US must consider creating an entity it. Organizational changes might include or be drawn from the approaches to government regulation and enforcement activities within those other domains. But any action must be taken with a mind to protect individual liberty of US citizens and our posterity, which is the reason for the US government's existence. How the US

[6] "The concept of commons is often understood to refer to resources shared among a group of people. The resources are typically classified by binaries such as (non-)natural, (non-)rival and (non-) substractable, and the analytical focus is placed on governance for sustainable management." Basu Soutrik, Joost Jongerden, and Guido Ruivenkamp, "Development of the Drought Tolerant Variety Sahbhagi Dhan: Exploring the Concepts Commons and Community Building," *International Journal of the Commons* 11, no. 1 (March 2017): 1, accessed 20 December 2020, https://www.thecommonsjournal.org/article/10.18352/ijc.673/.

Department of Defense (DoD) views those physical and other operating environments and the identified domains found within them is our starting place.

US Views on Authorities, Environments, and Domains

Unlike its competitors, US policy fails to see and therefore does not treat the Information Domain as an emergent holistic domain of action where US sovereignty must be protected. Instead, the US government treats the Information Domain as private parceled properties outside the sphere of legal action except in response to crime or foreign activity.[7] Additionally, current US government organizations that possess legal authority were created as regulatory bodies for criminal law. The regulation of cyberspace was only added to their mandates to protect confidentiality, availability, and integrity of information in the course of their original tasks.

The authorities for actors in cyberspace within US Code include but are not limited to Title 6 (Domestic Security) for Department of Homeland Security (DHS), Title 10 (Armed Forces) for DoD, Title 18 (Crimes and Criminal Procedures) for Federal Bureau of Investigation (FBI), Title 32 (National Guard), Title 34 (Crime Control and Law Enforcement) all Federal Law Enforcement, Title 44 (Telecommunications) Department of Commerce, and Title 50 (War and National Defense) DoD and the Intelligence Community.[8] This diffusion of authorities into other areas of focus helps manage those original tasks; however, it has created disparate regulatory frameworks to deal with specific Information Domain problems. The aforementioned Solarwinds SEC report, financial regulatory disclosure for corporations, is a demonstration of this problem.

[7] "The private sector owns about 80 percent of the Internet, which makes it difficult for the government to help protect our networks. Right now, if your house is broken into, you call 911, and the cops come. But if a company gets cyberattacked and billions of dollars are stolen -- which has happened in the United States, and it is happening--they cannot call a cyber-911 line in the same way." Admiral Michael Rogers, Director NSA/Commander USCYBERCOM, "Hearing of the House (Select) Intelligence Committee Subject: "Cybersecurity Threats: The Way Forward," National Security Agency Central Security Service, November 20, 2014, accessed 20 December 2020, https://www.nsa.gov/news-features/speeches-testimonies/Article/1620360/hearing-of-the-house-select-intelligence-committee-subject-cybersecurity-threat/.

[8] US Congress, "US Code Index," Office of Law Revision Counsel, accessed February 1, 2021, accessed 20 December 2020, https://uscode.house.gov/browse.xhtml.

The filing addresses the potential impact to shareholders but fails to address national security requirements, or rather when the national security implications are considered; the US government is now remediating an issue rather than defending against one. The system as designed ignores the need for monitoring the Information Domain for warning and defense. Instead, the US consistently responds to attacks trying to discern whether a foreign power has already maneuvered toward a *fait accompli* which ignores the Information Domain's emergent nature as an operating environment within a global commons as part of the public square in need of regulatory protections.

For the US government generally, the law is the basis for government and military regulatory and organizational action in any sphere of activity. Current regulatory and organizational measures do not address the Information Domain as such. Rather, the historical treatment of other environments by the US DoD also called domains, may inform the development of approaches to government regulation and enforcement activities in an emergent Information Domain. Ends however do not justify the means and from a strategic and constitutional perspective, any actions to regulate the Information Domain must be taken with a mind to protect individual liberty for ourselves and its posterity.

Current joint doctrine does not define the words environment or domain. Doctrinally, the joint force commander is assigned to an operating environment and finds themselves responsible for an area of operations. This environment includes elements of the physical domains: air, land, maritime, and space; the information environment, including the cyberspace domain; the electromagnetic spectrum; and other factors such as enemy, neutral, and friendly systems.

Given this description, the environment appears to be made up of domains and other entities residing within it. Though each of the physical domains is defined and has forces aligned to it, the joint doctrine states clearly that nothing in the definitions of a domain implies or mandates exclusivity, primacy, or command and control (C2) of that domain. This doctrinal explanation appears to be a means to ensure jointness and interoperability between military

services. The primacy warning also seems explicitly meant to ensure any assigned joint force commander retains the ability to enable C2 within his operating environment based upon the most effective use of available resources to accomplish assigned missions.[9]

Current joint doctrine for information operations defines the information environment as the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.[10] Under this doctrinal interpretation, the environment includes three elements, physical, informational, and cognitive. As defined, two of these elements, physical and informational include what joint doctrine defines as cyberspace.

The Physical Dimension includes all tangible elements, including communications systems, people, and the supporting infrastructure, enabling the environment. These elements include, but are not limited to, newspapers, books, cell-phone towers, data centers, all types of computers, i.e., laptops, smartphones, tablets, etc. A vital aspect of the physical dimension is identified in Joint Publication 3-13 as the physical dimension "is not confined solely to military or even nation-based systems and processes; it is a defused network connected across national, economic, and geographical boundaries."[11]

The Informational Dimension encompasses where and how information is collected, processed, stored, disseminated, and protected. It is the dimension where the C2 of military forces is exercised and where the commander's intent is conveyed. Actions in this dimension affect the content and flow of information.[12]

The Cognitive Dimension is the understanding of the environment found in the eye and mind of the beholder. It includes the minds of those who use information, which is every person

---

[9] US Department of Defense, Joint Staff, Joint Publication (JP) 3-0, *Joint Operations* (Washington, DC: Government Publishing Office, 2018), II-1.

[10] US Department of Defense, Joint Staff. Joint Publication (JP) 3-13, *Information Operations* (Washington, DC: Government Printing Office, 2014), I-2 to I-3.

[11] US Joint Staff, JP 3-13, (2014), I-2 to I-3.

[12] US Joint Staff, JP 3-13, (2014), I-2 to I-3.

in the world. So, it refers to individuals but also groups. How people and groups perceive and process information, their individual and collective understanding, judgments, and decision making are part of the cognitive. The cognitive is influenced by numerous factors, again including but not limited to individual and cultural beliefs, social norms, personal and institutional values, religion, politics, emotions, and experience. Joint Publication 3-13 contends, "As such, this dimension constitutes the most important component of the information environment."[13]

Current joint doctrine defines cyberspace as a domain within the information environment consisting of the interdependent networks of information technology infrastructure and the data residing and transiting those networks.[14] Similarly to the information mentioned above, doctrinally, the cyber domain includes three elements called layers, the physical, logical, and persona.

The Physical Layer consists of information technology and communications infrastructure. These elements store, transport, process, and present information and include what is commonly referred to as hardware and infrastructure (e.g., computing devices, storage devices, network devices, and wired and wireless links).[15]

The Logical Layer consists of the logic programming (code) that drives network components. It consists of multiple systems' ability to interact because of their programmed logical connections and enables data exchange or have data processing relationships not tied to a specific physical link or node. Though individual links and nodes are represented in this logical

[13] US Department of Defense, Joint Staff, Joint Publication (JP) 3-13, *Information Operations*, (Washington, DC: Government Publishing Office, 2014), I-2 to I-3.

[14] US Department of Defense, Joint Staff, Joint Publication (JP) 3-12, *Cyberspace Operations* (Washington, DC: Government Publishing Office, 2018), I-1 – I-4.

[15] US Joint Staff, JP 3-12, (2018), I-1 – I-4.

layer, it includes other distributed elements, including data, applications, presentation, and network processes.[16]

The Persona Layer is the collection of identities in cyberspace made up of digital representations of persons including, network or user accounts, whether they are actual humans or simply automated entities or bots. This layer also includes personas created by relationships between multiple accounts. Such identities are created when disparate data that is relatable to a specific user is aggregated across multiple platforms (e.g., e-mail and IP addresses, web pages, phone numbers, log-in information, including user IDs and passwords).[17]

The DoD's key point is that the holistic information environment is considered an integral part of the joint force commander's operating environment. A domain that the commander must operate in is part of his command responsibility to include establishing information dominance. So, if it exists as a domain for military operations, then it exists outside military operations. Further, as it is now a global environment due to information technology, it has become a target for adversaries to exploit and compete with the US.

Competitor Treatment of the Information Domain

The US *National Security Strategy* has shifted to a global competition view. We must explore how two of its key competitors view the Information Domain to understand existing competition. This understanding will assist in formulating US activity within the environment. Russia and China are the two competitors used for this study as they remain likely adversaries and are seen as peers or at least near peers on the global stage and named in the US National Defense Strategy.[18]

---

[16] US Joint Staff, JP 3-12, (2018), I-1 – I-4.

[17] US Joint Staff, JP 3-12, (2018), I-1 – I-4.

[18] US Department of Defense, *National Defense Strategy* (Washington, DC: Government Publishing Office, 2018), 2.

Russian authorities view information and cyberspace as inseparable and have long been paranoid concerning the spread of information. Since the Soviet Union's days, fears of both the security of information technology and control of content within its information environment are evident.[19] In the Internet age, Russia has continued its efforts to ensure the security of its information environment and cyber domain. Since the early 1990s, Russia has enacted a series of significant telecommunications laws under the acronym in English name System for Operative Investigative Activities (SORM).[20] The acronym is a transliteration of Система оперативно-разыскных мероприятий which in English means System for Operative Investigative Activities. These laws and regulations are the basis for legal monitoring of all telecommunications in Russia by the Federal Security Service (FSB). SORM gives the FSB capabilities the US would compare to its own National Security Agency (NSA) except in that NSA has to get a warrant from a court to gather and listen to US citizen communications. Russian telecommunications and Internet companies are legally required to install FSB equipment as monitoring of citizens' communications is expected in Russia.[21]

Since 2014, Moscow has sought to build on its SORM framework to enable better control over Internet-based communications. This includes a law declaring any blog with more than 3000 views as a media site, enabling the FSB to treat popular bloggers as media outlets and allowing

[19] "Copy Machines were strictly controlled in the Soviet Union from 1949 to 1989 to prevent the spread of malicious information." Michael Parks, "Soviets Free the Dreaded Photocopier," *Los Angeles Times*, October 5, 1989, accessed 20 December 2020, https://www.latimes.com/archives/la-xpm-1989-10-05-mn-913-story.html.

[20] N. Nikiforov, "Приказ Минкомсвязи Об Утверждении Правил Применения Оборудования Систем Коммутации, Включая Программное Обеспечение, Обеспечивающего Выполнение Установленных Действий При Проведении Оперативно-Розыскных Мероприятий [Order of the Ministry of Telecom and Mass Communications Concerning the Approval of the Regulations for the Use of Equipment for Switching Systems, Including Software, for the Implementation of the Specified Actions during Operative Investigative Activities]," Российская газета [Russian Gazette], July 18, 2014, accessed 20 December 2020, https://rg.ru/2014/07/18/kommutacia-dok.html.

[21] Andrew James Lewis, "Reference Note on Russian Communications Surveillance," Center for Strategic and International Studies, April 18, 2014, accessed 20 December 2020, https://www.csis.org/analysis/reference-note-russian-communications-surveillance.

censoring of speech deemed a national security threat.[22] The physical and logical organization of the Internet presented some technical challenges to enforcement, and the legal efforts by Moscow to control its segment of the Internet continue. In 2019 the Kremlin introduced new directives, a Sovereign Internet Law, creating a legal framework for state management of the Internet within Russia's borders. This consolidation of regulations and laws is meant to achieve three objectives. First, to enable mechanisms for effective Internet surveillance in Russian territory. Second to reinforce Moscow as the key regulator of the Internet in Russia. Thirdly Moscow seeks to establish a state-centered model of the Internet at the international level.[23] Moscow's legal actions clearly identify and connect information and cyberspace, as their efforts seek to control content.

Russia's published Information Security Doctrine and Military Doctrine clearly articulates the national view of information content as a potential national security and military threat:

> Intelligence services of certain States are increasingly using information and psychological tools with a view to destabilizing the internal political and social situation in various regions across the world, undermining the sovereignty and violating the territorial integrity of other States. Religious, ethnic, human rights organizations and other organizations, as well as separate groups of people, are involved in these activities, and information technologies are extensively used towards this end.[24]

Russian military doctrine identifies a shift in military threats to the information sphere, including the use of information and communication technologies for military-political purposes.[25] The

[22] Famil Ismailov, "Russia Enacts 'Draconian' Law for Bloggers and Online Media," *BBC News*, July 31, 2014, accessed 20 December 2020, https://www.bbc.com/news/technology-28583669.

[23] Alena Epifanova, "Deciphering Russia's 'Sovereign Internet Law:' Tightening Control and Accelerating the Splinternet," *DGAP Analysis*, no. 2 (January 2020): 1-11.

[24] Vladimir Putin, "Russian Federation Armed Forces' Information Space Activities Concept," Ministry of Defence of the Russian Federation, accessed December 15, 2020, accessed 20 December 2020, https://eng.mil.ru/en/science/publications/more.htm?id=10845074%40cmsArticle.

[25] Vladimir Putin, "Military Doctrine of the Russian Federation," Diplomacy Online, December 25, 2014, accessed 20 December 2020, https://rusemb.org.uk/press/2029.

organization and resourcing of the Russian military account for this and clearly enables military action in the information sphere to protect Russian interests.

Coincidental to that mentioned shift of military threats, Moscow established its National Guard in 2016, combining multiple elements of interior ministry law enforcement and security elements. This presidential order effectively created a new military force in Russia which includes mechanized brigades and divisions, special troops, and an air force. In 2017 the National Guard reportedly began hiring for what was called a new intelligence unit looking for people with technical qualifications to monitor online activity for extremists,[26] though official statements from the National Guard denied the reports.[27] Regardless the consolidation of internal law enforcement capabilities with a military organizational structure and capabilities for internal security echoes the days of the Russian secret police, and given Moscow's history of efforts to control the sharing of information, it would be naïve to think that the National Guard has no capabilities or authorities to operate in the information sphere.

Moscow's external view on information security identifies the nature of the problem, which it sees as not only technological but also as political in nature. Its solution is sovereignty, more specifically, national sovereignty.[28] In its 2013 state policy on international information security, Moscow calls out the need for the development of regional systems and the formation of a global system of international information security. It goes on to identify the need for recognized principles and norms, explicitly calling for respect for state sovereignty.[29] Russia's

[26] Sergey Sukhankin, "Russian National Guard: A New Oprichnina, 'Cyber Police' or Something Else?," The Jamestown Foundation, March 21, 2017, accessed 20 December 2020, https://jamestown.org/program/russian-national-guard-new-oprichnina-cyber-police-something-else-2/.

[27] Dimitriy Rogulin, "Russia's National Guard Rejects Media Reports about Establishing Cyber Intelligence," TASS, March 16, 2017, accessed 20 December 2020, https://tass.com/politics/935846.

[28] Pasha Sharikov, "Understanding the Russian Approach to Information Security," *European Leadership Network*, January 16, 2018, accessed 20 December 2020, https://www.europeanleadershipnetwork.org/commentary/understanding-the-russian-approach-to-information-security/.

[29] Vladimir Putin, "Основы Государственной Политики Российской Федерации в Области Международной Информационной Безопасности На Период До 2020 Года [The Information Security

outreach effort acting on these goals includes diplomacy, academia, and commercial efforts to garner support for its proposals. This includes participation in United Nations (UN) efforts, specifically the United Nations Group of Government Experts, regional groups such as the Shanghai Cooperation Organization, and security cooperation groups, primarily Brazil, Russia, India, China, and South Africa (BRICS).

China's view of information and cyberspace is similar but somewhat more clouded than Russia's. Beijing's actions in law, policy, and military doctrine indicate it also sees the information environment and cyber-domain as linked. Unlike Russia, whose approach focuses more on making illegal actions in the domain, China has gone to great lengths to limit access to its information environment by the rest of the world as a means of control. The Great Firewall, the most infamous tool of this isolation effort,[30] has come to be synonymous with censorship in the Western world. It is not a singular object, however, and actually represents a legal, regulatory, and hardware collection designed to control the content of information Chinese citizens are able to view when they access the Internet. Beijing's approach to the Information Domain is focused on its people.

The release of World Wide Web and Hypertext Transfer Protocols in 1994 in effect created the modern commercial Internet.[31] The number of Internet users in China from 1994 to 2017 has grown from about 15,000 to nearly 800 million (see Figure 1).[32] The pervasive growth

---

Policy of the Russian Federation for the Period up to 2020]," Совет Безопасности Российской Федерации [Security Council of the Russian Federation], July 24, 2013, accessed 20 December 2020, http://www.scrf.gov.ru/security/information/document114/.

[30] Danny O'Brien, "China's Global Reach: Surveillance and Censorship Beyond the Great Firewall," Electronic Frontier Foundation, October 10, 2019, accessed 20 December 2020, https://www.eff.org/deeplinks/2019/10/chinas-global-reach-surveillance-and-censorship-beyond-great-firewall.

[31] Felicity Sheppard, "The Internet over the Past 20 Years," *ABC News Australia*, May 27, 2014, accessed 20 December 2020, https://www.abc.net.au/news/2014-05-25/internet-changes-over-20-years/5470442?nw=0.

[32] Max Roser, Hannah Ritchie, and Esteban Ortiz-Ospina, "Internet," Our World in Data.org, July 14, 2017, accessed 20 December 2020, https://ourworldindata.org//internet.

of Internet use in China was matched by government efforts to curate and control content. Like any growing effort, the effectiveness of censorship and control vary throughout the country. According to media reports, online censors in China have grown in the past few years from what was 30-40 employees to nearly a thousand people reviewing and auditing content.[33]

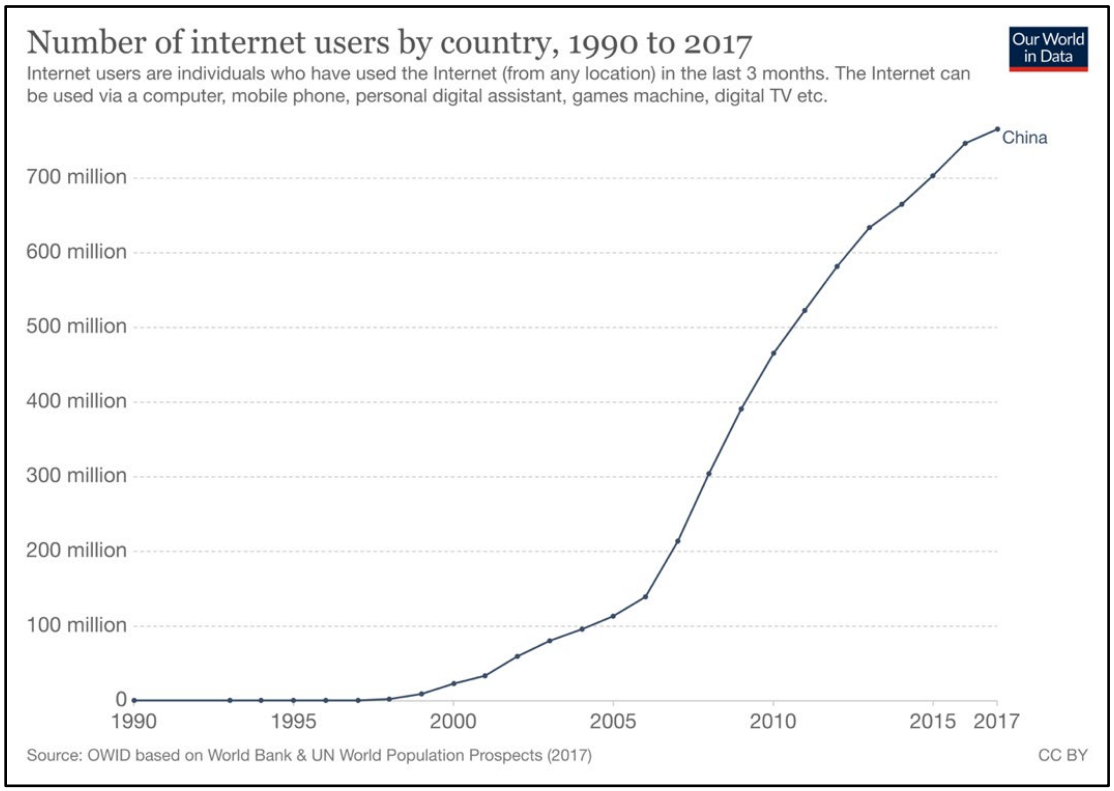

Figure 1. The Growth of Internet Users in China 1990-2017. Max Roser, Hannah Ritchie, and Esteban Ortiz-Ospina, "Internet," Our World in Data.org, July 14, 2017, https://ourworldindata.org/internet.

The Great Firewall forms a perimeter for the regime around its Information Domain, enabling blocking of access to content from abroad. It is the means by which Beijing stops its citizens and anyone else living in China from accessing foreign web content. Chinese authorities have equipment at each of the country's global Internet gateways enabling the filtering and

[33] Cate Cadell and Pei Li, "Tea and Tiananmen: Inside China's New Censorship Machine," *Reuters*, September 29, 2017, accessed 20 December 2020, https://www.reuters.com/article/china-Congress-censorship/tea-and-tiananmen-inside-chinas-new-censorship-machine-idUSL4N1LW25C.

blocking of content associated with either websites or keywords.[34] All of these steps enable automated policing of the Information Domain for Beijing.

Chinese information security law is focused on the use of legal use of communications technology in general, similar to the US. There are, however, in individual sections of the law, a clear effort to control user actions and effectively criminalize forbidden content. Article 68 of the Chinese security law identifies penalties for such prohibited activities as the use of banned content on the Internet, which though not "criminal," are seen as violations and impact the violator's social credit score.[35]

The social credit score is another part of China's efforts to regulate and control its Information Domain and control content precisely. The social credit score is, in effect, a carrot and stick approach to nudge Chinese citizens toward Beijing's preferred behaviors within the domain. Social credit scoring is actually a system of systems. Relying on multiple datasets, including but limited to financial, online activity, legal, social interactions, and travel history, the social credit score is linked to a system of rewards and punishments meant to shape behavior and minimize dissent and fraud.[36] Chinese citizens who pay their debts, and municipal fines, keep to the government preferred social circles, and refrain from posting or reading objectionable content online have higher scores and can earn rewards from the government, say scholarships for their children or the ability to travel abroad. Failure to do those things, however, can cause a person to be blacklisted. In one infamous example, a lawyer from Beijing was blacklisted for an "insincere"

[34] Olesya Tkacheva, Lowell H. Schwartz, Martin C. Libicki, Julie E. Taylor, Jeffrey Martini, and Caroline Baxter, *Internet Freedom and Political Space* (Santa Monica, CA: RAND Corporation, 2013), 97-98.

[35] Rogier Creemers, Paul Triolo, and Graham Webster, "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," New America, June 29, 2018, accessed 20 December 2020, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

[36] Charlie Campbell and Cheng Du, "How China Is Using Big Data to Create a Social Credit Score," *Time Magazine*, August 14, 2019, accessed 20 December 2020, https://time.com/collection/davos-2019/5502592/china-social-credit-score/.

court apology, resulting in him being stranded 1,200 miles from home and unable to buy a train ticket for travel within China.[37] Chinese cybersecurity law clearly states any violation shall be put into credit records and made public.[38]

China's social interactions are captured in the Information Domain through a system of mass surveillance. China is a global leader in what is called smart city initiatives. The networking of sensors, metering devices, cameras, and monitoring capabilities connected to big-data processing with artificial intelligence analysis to enable the management of cities.[39] Using this capability domestically, China is able to connect the actions of its people to the Information Domain. It also is able to export this potential population control capability abroad as well.

Much like the United States, China's military doctrine reflects a recognition of the cyber domain. Since 2004 the People's Liberation Army has incorporated the term Informatized Warfare as a key principle in its military doctrine. This appears to be a reflection of the US military principle of Joint military operations in a coordinated C4ISR concept.[40] This is believed to include the use of cyberspace operations, and in the 2014 iteration included the winning of localized informatized wars and Military Operations Other than War, a doctrinal term the US used in the mid-1990s.[41]

China's 2015 Military Strategy clearly articulates the military nature of cyberspace. Indeed, the translated strategy similar to the military doctrine reflects the US's own strategy. It

---

[37] Maya Wang, "China's Chilling 'Social Credit' Blacklist," *Human Rights Watch*, October 28, 2020, accessed 20 December 2020, https://www.hrw.org/news/2017/12/12/chinas-chilling-social-credit-blacklist#.

[38] Creemers, Triolo, and Webster, "Translation: Cybersecurity Law of the People's Republic of China," Articles 9 and 12.

[39] Katherine Atha, Jason Callahan, John Chen, Jessica Drun, Ed Francis, Kieran Green, Dr. Brian Lafferty, Joe McReynolds, Dr. James Mulvenon, Benjamin Rosen, and Emily Walz, "China's Smart Cities Development" (Research Report prepared on behalf of the US-China Economic and Security Review Commission, SOS International, Vienna, VA, 2020).

[40] Bekir Ilhan, *China's Evolving Military Doctrine After The Cold War* (Washington, DC: SETA, 2020), accessed 20 December 2020, https://setav.org/en/assets/uploads/2020/02/A56En.pdf.

[41] US Department of Defense, Joint Staff, Joint Publication (JP) 3-07, *Joint Doctrine for Military Operations Other Than War* (Washington, DC: Government Printing Office, 1995).

recognizes the strategic nature of cyberspace as well as its role in economic and social development as a domain of national security. Additionally, Beijing's strategy speaks to cyberspace as an arena of strategic competition with a growing number of cyber military forces. The strategy finishes the discussion of cyberspace by including other standard issues, including threats infrastructure, international cooperation, development of cyber military capability.[42]

China, like Russia, advocates for the establishment of state sovereignty and policies of non-interference in cyberspace. They are a participant in the BRICS international information security efforts, as well as those of the Shanghai Cooperation Organization. China remains averse to extending the United Nations (UN) Charter and Law Relating to Use of Military Force to cyberspace activities. However, the UN Group of Government Experts made clear the potential applicability of the UN Charter to cyberspace in 2013. However, any progress toward an international understanding remains stalled as some countries, including China, remain reluctant to formalize specific terms for fear of conceding possible advantages they currently possess.

United States Defense of the Information Domain

> Congress shall make no law respecting an establishment of religion or prohibiting the free exercise thereof, or abridging the freedom of speech, or of the press, or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.
>
> —US Constitution, Amendment I

The United States was founded on the idea that every individual possesses inalienable rights, and its union was created to secure liberty for today and tomorrow. Providing for the common defense is part of its purpose, as well as the promotion of the general welfare. Just as

[42] The State Council Information Office of the People's Republic of China, *China's Military Strategy* (Beijing, 2015), 16-17, Jamestown.org, accessed September 15, 2020, https://jamestown.org/wp-content/uploads/2016/07/China%E2%80%99s-Military-Strategy-2015.pdf.

Clausewitz identified the political nature of Napoleon's revolution[43] as a key to the military success to France and Isserson identified the Soviet Revolution as an underpinning for Soviet military reforms and organization used to defeat Germany in WWII,[44] the United States must understand and continue to consider its own revolution as it seeks to protect its people's liberty and individual rights from threats within the Information Domain.

The current state of US regulation within the Information Domain started as early as 1798 with the passing of four laws known as the Alien and Sedition Acts.[45] These laws sought to curtail sedition and extended naturalization of citizens from five to fourteen years as part of an effort to prevent war between the US and France. They are viewed as a foundational part of free speech regulation and have shaped legal precedents to this day.

Obscenity, public safety, and fraud are the other areas of law where the US regulates the content side of the Information Domain. These areas seek to protect public decency and the rights of individuals from harm through false statements or misrepresentation. Such laws are the sources of many standard features in American society, some government-mandated, and others created by industries themselves. It was the government, for example, that required Surgeon General warning labels on cigarettes in 1969, while the entertainment industry self-regulated creating movie ratings in 1968 and video game content warnings in 1994.

As far as the regulation of cyberspace goes, the US government essentially created the Internet for national defense purposes, which at the outset at least ensured an insider level

---

[43] Carl Von Clausewitz, *On War*, ed. and trans. Howard Michael and Peter Paret (Princeton, NJ: Princeton University Press, 1984), 609.

[44] G. S. Isserson, *The Evolution of Operational Art*, trans. Bruce Menning (Fort Leavenworth, KS: Combat Studies Institute Press, 2013), 7-14.

[45] Douglas E. Lee, "Seditious Libel," *The First Amendment Encyclopedia*, October 2016, accessed December 15, 2020, https://www.mtsu.edu/first-amendment/article/1017/seditious-libel#:~:text=Congress%20criminalized%20seditious%20libel%20in%201798&text=In%201798%20Congress%20passed%20four,the%20government%20or%20its%20officials.

understanding of that part of the environment.[46] The Advanced Research Projects Agency Network (ARPANET) pioneered network sharing of digital systems and data between computers across the United States. Conceived and built in the late 1960s, this led to the Internet as it is today. The first instance of "securing" this computer network occurred in 1975 when the management of ARPANET was transferred to the Defense Communications Agency and the systems security officer created rules such as "only military personnel or ARPANET sponsor-validated persons working on government contracts or grants may use the ARPANET."[47] These rules, however, were largely ignored by ARPANET users. Cybersecurity began imperfectly and remains to this day a challenge with ever escalating requirements.

In 1991 Congress passed the High-Performance Computing Act,[48] a law that led to the broad commercialization of computer networking through government investment in infrastructure, including fiber optic cables creating the backbone of the Internet. This act enabled widespread commercialization of the Internet. What had been US Government funded research and development in communications became ever growing commercial information technology allowing the sharing of data and revolutions in commerce globally.

That creation and growth of computer networking also impacted crime and espionage. Computer-based commerce created new possibilities for theft and fraud. The conversion of large volumes of information to data on electronic media and the ability to access and to pass information over a data connection at the speed of light did the same for spies. The first espionage

[46] Navarria Giovanni, "How the Internet Was Born: From the ARPANET to the Internet," The Conversation, November 2, 2016, accessed 20 December 2020, https://theconversation.com/how-the-internet-was-born-from-the-arpanet-to-the-internet-68072.

[47] Ibid.

[48] US Congress, "S.272 - High-Performance Computing Act of 1991," Congress.gov, December 9, 1991, accessed 20 December 2020, https://www.Congress.gov/bill/102nd-Congress/senate-bill/272.

hack of note of ARPANET systems was a series of unauthorized accesses by a German operative in the late 1980s, who then sold what he found to the Soviet Committee for State Security.[49]

Throughout the 1990s and early 2000s, the rapid commercial growth of Information technologies impacted almost every aspect of global life, including advances in military communications and operations. In the US, the recognition of cyber as a domain of military action evolved to a point in 2009 where consolidation of military capabilities for that domain was vested into US Cyber Command, a sub-unified command within US Strategic Command at its outset. By 2017 US Cyber Command was elevated to a full combatant command, and as of 2020, it recognizes the inherent mission-related connections between cyber and information content creating the Information Domain.[50]

These connections are more and more impacting national security and people's rights to free speech and free association. People are sharing information online, including content viewed by some as misinformation or disinformation. The controversies surrounding election interference stories in 2016, 2018, and 2020 are prominent examples. In each case, claims were made concerning foreign interference with disputed content as primary evidence of nefarious actions, followed by assurances from government officials that there were either no efforts to hack actual voting infrastructure or that any such efforts were unsuccessful.[51]

Most recently, the Senate Judiciary Committee initiated hearings concerning censorship by social media companies associated with the 2020 elections.[52] Additionally, there is anecdotal

---

[49] Clifford Stoll, *The Cuckoo's Egg: Inside the World of Computer Espionage* (New York: Doubleday, 1989).

[50] US Cyber Command, "US Cyber Command History," US CYBERCOM, accessed February 9, 2021, accessed 9 February 2021, https://www.cybercom.mil/About/History/.

[51] Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation, "Internet Crime Complaint Center (IC3): False Claims of Hacked Voter Information Likely Intended to Cast Doubt on Legitimacy of US Elections," Internet Crime Complaint Center (IC3), September 28, 2020, accessed 20 December 2020, https://www.ic3.gov/Media/Y2020/PSA200928.

[52] Cat Zakrzewski and Rachel Lerman, "The Election Was a Chance for Facebook and Twitter to Show They Could Control Misinformation. Now Lawmakers Are Grilling Them on It," *The Washington*

evidence of political bias in social media, which would be the same sort of national security issue that occupied so much political will, government resources, and media attention for the actions of Russia in the 2016 election.[53] However, the focus of regulation remains on cybersecurity with no effort to address the impact or regulation to prevent manipulation of information, censorship by commercial entities, and foreign influence outside of making political points. Reluctance to accept a need for regulation concerning such content is the issue. The CEO of Facebook, Mark Zuckerberg, in 2019 identified the need for regulation of the Internet for the purposes of controlling harmful content, election integrity, privacy, and data portability.[54] Considering the recent calls for unity, individual liberty, common defense, and promoting the general welfare the US needs privacy to be emphasized as the basis for discussion.

Factors Affecting US Authorities

Protection of liberty and of individual human rights are at the core of factors shaping US legal authorities to regulate and act within the information environment. The First and Fourth Amendments to the US constitution expressly limit government actions toward curtailing freedom of expression and the conduct of unreasonable search and seizure in violation of privacy. Additionally, the principle of separation of powers inherent in the US model of government results in disparate levels of jurisdiction and the evolution of legal authorities to act to address "unsafe" activity viewed as in need of regulation as it is identified.

Take, for example, the regulation of drones. Small remote piloted drones have been available for years now. In the past ten years proliferation of inexpensive models equipped with cameras has enabled their use to film subjects, providing some fantastic video and still images.

Post, November 17, 2020, accessed 20 December 2020, https://www.washingtonpost.com/technology/2020/11/17/tech-hearing-dorsey-zuckerberg/.

[53] James Clapper, ICA 2017-01, *Assessing Russian Activities and Intentions in Recent US Elections* (Washington, DC: Director of National Intelligence, 2017).

[54] Mark Zuckerberg, "Four Ideas to Regulate the Internet," Facebook, March 30, 2019, accessed 20 December 2020, https://about.fb.com/news/2019/03/four-ideas-regulate-internet/?utm_source=ads.

This sort of photography can support hobbyists, be commercialized, or help targeting for extremists. The regulatory reaction to this technology includes FAA rules and licensing for the hobbyist and commercial users including creation flight plans and gaining FAA approval for them, and future requirements for flight transponders for recreational drones,[55] as well as local no-drone zones.[56] This light-touch approach, adding requirements incrementally over time, is endemic to the US regulatory and legal system.

The NSA and DoD offer another example. They possess the greatest capability to monitor and collect information, however their authority to use that capability falls within either Title 50 for intelligence collection or Title 10 for national defense in war. Though they can collect and monitor for foreign threats, they are specifically limited as to how such data can be used or revealed. According to a 2018 *New York Times* report, the NSA collected more than 534 million records of phone calls and text messages from American telecommunications providers.[57] There are restrictions on the use of those records under existing intelligence oversight regulations to protect citizens' privacy. Following the prohibition on bulk phone data collection in 2015, Congress authorized the call detail records program as a means of preserving a collection technique called contact-chaining. Contact chaining allows review of data for patterns between the contacts of a surveillance target phone calls both outgoing and incoming. This reduced the scale of collection from bulk collection which gathered all call data and meta data. Contact chaining not only allows NSA to collect the phone records of a single target, but also the phone records connected to the target up to "two hops out." The first hop being the phone records of

[55] Federal Aviation Administration, "FAADroneZone," US Department of Transportation, December 28, 2020, accessed 28 December 2020, https://faadronezone.faa.gov/#/.

[56] W. J. Hennigan, "Pentagon Establishes No Drone Zone for Recreational UAVs," Government Technology, April 1, 2016, accessed 20 December 2020, https://www.govtech.com/public-safety/Pentagon-Establishes-No-Drone-Zone-for-Recreational-UAVs.html.

[57] Charlie Savage, "N.S.A. Triples Collection of Data From US Phone Companies," *The New York Times*, May 4, 2018, accessed 20 December 2020, https://www.nytimes.com/2018/05/04/us/politics/nsa-surveillance-2017-annual-report.html.

those numbers that the target called or those that called the target. The second hop being the records of those called by or who called numbers in the first hop.[58] It is not as wide a net as bulk collection, but it remains a wide net nonetheless. In order to monitor US citizens in general there would need to be a repurposing of existing DoD or NSA resources which are already focused on monitoring foreign military threats. Diverting resources to monitor the US Information Domain beyond the just cyberspace risks a distraction from original purpose of signals intelligence in support of existing DoD missions.

The FBI also possesses capability to monitor networks. In 2017 testimony Scott Smith, head of the FBI Cyber Division, stated that the FBI was working with the intelligence and law enforcement community to address cyberthreats. He specifically said "The information domain is an inherently different battle space, requiring government bureaucracies to shift and transform to eliminate duplicative efforts and stovepipes and move toward real-time coordination and collaboration to keep pace with the growing threat."[59] Though the FBI understands the problems of the Information Domain, their capability is designed for criminal investigation, not for monitoring the information space for threats.

Legal Concerns

The US sees respect for the rule of law as one of the international norms integral to global cooperation in cyberspace. The Cyberspace Solarium Commission (CSC) Report highlights American Leadership in shaping international standards of behavior as essential to the US strategy for defense in cyberspace.[60] The application of both domestic and international law

[58] Jake Laperruque, "The History and Future of Mass Metadata Surveillance," Project On Government Oversight, June 11, 2019, accessed 20 December 2020, https://www.pogo.org/analysis/2019/06/the-history-and-future-of-mass-metadata-surveillance/.

[59] Scott Smith, "Roles and Responsibilities for Defending the Nation from Cyber Attack," Statement before the Senate Armed Services Committee, October 19, 2017, accessed 20 December 2020, https://www.fbi.gov/news/testimony/cyber-roles-and-responsibilities.

[60] Angus King and Mike Gallagher, *United States of America Cyberspace Solarium Commission* (Washington, DC: Government Publishing Office, 2020), 3.

to the Information Domain is a crucial point of contention to cooperation within the domain. Like the Solarium Report, other international groups such as the UN Group of Government Experts and NATO have emphasized the significance of international law and the principle of national sovereignty as the basis for cooperation and mutual security. Cooperation among nations below the level of war to avoid escalation to conflict is a crucial aspect of the policy, as is an understanding of how the law applies in the emergent Information Domain.

The NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) was established in the wake of cyber-attacks against Estonia linked to Russian actors. Since 2009, the CCDCOE holds an annual cybersecurity conference focusing on legal and technological aspects of cyber-conflict. Its primary publication, the Tallinn Manual, is viewed as one of the most comprehensive analyses of how existing legal concepts apply to cyberspace.[61]

The Tallinn Manual 2.0 provides a good starting point for exploration of the extension and applicability of existing law to information activities. The two areas of specific focus for this paper are those of sovereignty and jurisdiction, areas where the US could find potential areas of cooperation with other states. How sovereignty applies to the Information Domain helps determine how nations organize to defend and conduct themselves within agreed-upon frameworks of international law.[62] Individual states have different theories concerning how sovereignty applies explicitly to cyberspace. Some states, Russia and China mainly, include cognitive and information content as integral with the physical aspects of cyberspace, seeking to have restrictions on speech as part of the sovereignty discussion. They argue that state sovereignty extends to the protection of the people subject to the state and their culture.[63] This

[61] CCD COE, "About Us," CCD COE, accessed December 20, 2020, https://ccdcoe.org/about-us/.

[62] Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge: Cambridge University Press, 2016).

[63] James S. Phillips, "The Rights of Indigenous Peoples under International Law," *Global Bioethics* 26, no. 2 (2015): 120–27, doi:10.1080/11287462.2015.1036514.

suggests the informational and cognitive dimensions are also subject to sovereignty and linked to sovereign states in the same way as cyberspace infrastructure is as part of the physical dimension.

This point raises the topic of jurisdiction and precisely how it might apply to the information environment (physical, informational, and cognitive dimensions) in light of the applicability of national sovereignty within a domain where conversations among citizens of multiple countries on forums linked to a specific country are occurring in an arguably international grey zone.[64]

Jurisdiction falls into three basic categories of action: legislative, executive, and judicial. It is generally limited to territorial boundaries with some exceptions and refers to the authority of a state to dispense the full scope of law: civil, administrative, and criminal. Jurisdiction can be divided into two categories, territorial and extraterritorial. Territorial jurisdiction includes those actions within the boundary of a state and is relatively straightforward. Sovereign states within their borders exercise all three jurisdictional competencies. They write, execute, and make judgments inside their territory.[65]

Extraterritorial jurisdiction is where definitions get complicated. Concerning cyberspace, there is the circumstance when legislative and judicial jurisdiction can be applied extraterritorially, through actions such as sanctions and judgement in lawsuits, while the application of executive jurisdiction, in the form of enforcement, controversy can ensue due to inability to enforce such actions due to the nature of cyberspace and sovereignty. In theory, the physical location from which a cyber-crime originates would be the executive or enforcement jurisdiction. Lack of cooperation for extradition or agreement on what constitutes a crime in

[64] John A. Ragosta, "The Information Revolution--Culture and Sovereignty--a US Perspective," *Canada-United States Law Journal* 24 (January1998.): 155, accessed 20 December 2020, http://search.ebscohost.com.lumen.cgsccarl.com/login.aspx?direct=true&db=lgh&AN=1774434&site=ehost-live&scope=site; Michael N. Schmitt and Liis Vihul, "Respect for Sovereignty in Cyberspace," *Texas Law Review* 95 (2017): 1639-70.

[65] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 15-18.

cyberspace complicate the issue, as the US is not going to arrest or extradite anyone for defaming Russian President Putin in a meme. However, consider a case of theft, stealing property is near universally seen as a crime. Normally legal jurisdiction for arrest and prosecution is at the physical location of the theft. However, in cyberspace, where the thief and victim are in different countries the law is forced to consider the online locations for actions and potential jurisdictions which may be in effect. There a potentially multiple jurisdictional cases to be made by any country whose cyberspace infrastructure was traversed, i.e., whose territory was used in the commission of the crime (See Figure 2). Crime in cyberspace, as demonstrated, crosses many territorial jurisdictions. As such, in cyberspace, *inter alia*, extraterritorial jurisdiction can be applied to cyberspace.

Figure 2. Consider a cyber-crime committed FROM Asia, THRU Europe, TO North America. illustrates the concept of multiple jurisdictions. *Source* created by author.

US freedom of speech principles and the application of jurisdiction to the information aspects of the domain are problematic. Who has jurisdiction for online content? Is it at the point of creation or at where it is published, and the information content is consumed by other people? The UN Universal Declaration of Human Rights guarantees freedom of expression.[66] As does the

[66] George Washington, "The Constitution of the United States: A Transcription," National Archives and Records Administration, May 4, 2020, accessed 20 December 2020, https://www.archives.gov/founding-docs/constitution-transcript.

US Constitution guarantee freedom of speech.[67] Interestingly, the UN Declaration also explicitly endorses freedom of opinion.[68] If individuals possess these rights it suggests jurisdiction is not at the point of creation but at the point of publication. Any consideration of extraterritorial jurisdiction (specifically legal enforcement actions pertaining to the informational and cognitive dimensions within the Information Domain, including cyberspace), therefore - even considering sovereign territorial law - must also consider human rights as identified under the UN Declaration.

Sedition and libel laws are the traditional legal means of regulating information content by sovereigns, and even the US has sedition law as part of its criminal code.[69] The question becomes the application of such laws for actions in cyberspace. For example, the desecration of the king in Thailand is a serious crime.[70] Article 112 of Thailand's criminal code states, "Whoever, defames, insults or threatens the King, the Queen, the Heir-apparent or the Regent, shall be punished with imprisonment of three to fifteen years."[71] Enforcement of this law since its inception in 1908 has remained relatively stable and strict, with its spirit being included in the Thai constitution. Though there is little question about the territorial enforcement of such a law, the question for this papers purpose is how would extraterritorial jurisdiction be applied to actions on the Internet? In 2015, the Russian media agency which regulates Internet content in Russia, Роскомнадзор, made it illegal to publish Internet memes that depict a public figure in a way

[67] René Cassin, "Universal Declaration of Human Rights," United Nations General Assembly, December 10, 1948, accessed 20 December 2020, https://www.un.org/en/universal-declaration-human-rights/.

[68] Washington, "The Constitution of the United States: A Transcription."

[69] Roy S. Gutterman, "Sedition Laws and Free Speech," Jurist, Legal News and Commentary, May 14, 2015, accessed 20 December 2020, https://www.jurist.org/commentary/2015/05/roy-gutterman-sedition-laws/.

[70] Gavin Allen, ed., "Lese-Majeste Explained: How Thailand Forbids Insult of Its Royalty," *BBC News*, October 6, 2017, accessed 20 December 2020, https://www.bbc.com/news/world-asia-29628191.

[71] Thailand Lawyer, "Thailand Law Library," Thailand Law Library RSS, accessed December 15, 2020, accessed 20 December 2020, https://library.siam-legal.com/thai-law/criminal-code-royal-family-sections-107-112/.

contrary to the figure's "personality."[72] Though many countries have attempted to censor and limit access to online content arguably to maintain internal stability, it seems beyond reason for enabling fines or, in the extreme extradition, for the creation of an internet meme.

The question of extraterritorial jurisdiction creates a dilemma for the US as the first amendment protects online speech, which may be illegal in other countries. US protections for privacy can also be problematic as often in the US; there are no government-imposed requirements for establishing an online account as the source of such contested speech. The US barely polices its own citizens' speech online and is not organized or prepared to take on such a role to assist other countries' efforts. Further, in not policing its own space, the US leaves its own information space open to every sort of action, including foreign influence and global corporate influence and censorship.

The hands-off approach by the US, which effectively cedes the Information Domain to all actors, enables actions now considered a potential national security threat. Although the US Intelligence Community does some monitoring to identify foreign influence efforts, the US legal system restricts its action due to oversight restrictions, posing legal hurdles on the use of the Intelligence Community to spy on US citizens, which extend to the online US Internet platforms. That said, the DHS has developed cooperation agreements with some platforms to identify terrorism and online radicalization. This initiative indicates that monitoring of corporate networks and platform back-ends would be more effective in identifying and possibly curtailing foreign influence efforts. Having a regulatory or law enforcement capability outside the intelligence community for such an effort would assist in alleviating intelligence oversight concerns.

[72] Caitlin Dewey, "Russia Just Made a Ton of Internet Memes Illegal," *The Washington Post*, April 10, 2015, accessed 20 December 2020, https://www.washingtonpost.com/news/the-intersect/wp/2015/04/10/russia-just-made-a-ton-of-internet-memes-illegal/.

Mission Concerns

It is a misuse of the Intelligence Community, whose mission is gathering foreign intelligence, to counter foreign influence within the US information environment. Operationally the Intelligence Community collects information in ways that frequently break the laws of other nations. This moral ambiguity is accepted by the US public as part of the national defense mission, though there are strong caveats concerning protecting the civil liberties of US citizens and preventing of the politicization of intelligence. Prominent controversies include the weapons-of-mass-destruction reporting based on intelligence failures in deconfliction of between intelligence disciplines of human intelligence and geo-spatial intelligence sources that led to the US invasion of Iraq in 2003.[73] That error resulted in a review by the Senate of all Intelligence Community assessments associated with Iraqi Weapons of Mass Destruction[74] and lead to reforms within the Intelligence Community based on the 9/11 commission report.[75] Additionally "whistleblower" cases, such as those of NSA Contractor Edward Snowden[76] and US Army Soldier Chelsea Manning[77] cases, highlight alleged abuses or misuses of capability within the Intelligence Community and military.

These mission concerns about military and intelligence operations within the information environment and the cyber domain link back to human rights concerns and First and Fourth

---

[73] Bob Drogin, *Curveball: Spies, Lies, and the Man behind Them: The Real Reason America Went to War in Iraq* (London: Ebury, 2008).

[74] Select Committee on Intelligence, "Report of the Select Committee on Intelligence on the US Intelligence Community's Prewar Intelligence Assessments on Iraq," July 2004, accessed December 20, 2020, https://www.Congress.gov/108/crpt/srpt301/CRPT-108srpt301.pdf.

[75] Philip Shenon, "House Passes Bill to Overhaul US Intelligence System," *The New York Times*, December 7, 2004, accessed 20 December 2020, https://www.nytimes.com/2004/12/07/politics/house-passes-bill-to-overhaul-us-intelligence-system.html.

[76] Margaret Morris and Gary Bennett, "Edward Snowden and the Defence of Privacy," *The Guardian*, October 20, 2019, accessed 20 December 2020, https://www.theguardian.com/world/2019/oct/20/edward-snowden-and-the-defence-of-privacy.

[77] Sarah Childress, "Bradley Manning Sentenced to 35 Years for WikiLeaks," *Public Broadcasting Service*, August 21, 2013, accessed 20 December 2020, https://www.pbs.org/wgbh/frontline/article/bradley-manning-sentenced-to-35-years-for-wikileaks/.

Amendment issues. Freedom of speech is essential to discourse and guaranteed to Americans in the Constitution, but also to people in general as recorded in the UN Universal Declaration of Human Rights.[78] Communicating online has facilitated conversation on a global scale. It has created a commercial opportunity but has also concerns over criticism used as sedition and affecting the stability of governments. All nations, including the United States, have some restrictions on speech. In the US for example calls to action which result in physical harm or criminal activity are prosecutable offenses.[79] The sovereign state approach to internal regulation remains the preferred model for action globally. Respect for national sovereignty remains essential to cooperation among nations. This includes the need for US respect of its competitors and their own laws and rules. The US approach to the Information Domain in this construct has limited regulatory actions to ensure the confidentiality, availability, and integrity of data. This is more commonly referred to as cybersecurity.[80]

The intrinsic connection between the information environment and the cyber domain further complicates these issues. A current example can be seen in discussion related to social media content, specifically focused on Section 230 of the Communications Decency Act of 1996 This act is regulated by the Federal Communications Commission (FCC) and was not created for the internet, but rather to ensure pornography was not publicly broadcast on television.[81] Section 230 of the act was an effort to modify and apply regulations for broadcast television to computer

[78] Cassin, "Universal Declaration of Human Rights." "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

[79] Calvin Woodward, "2 Impeachment Trials, 2 Escape Hatches for Donald Trump," Associated Press, February 14, 2021, accessed 14 February 2021, https://apnews.com/article/donald-trump-trials-coronavirus-pandemic-mitch-mcconnell-elections-4d1d7ec837c3e942dcbfda962a6dd691.

[80] Pesante Linda, "Introduction to Information Security," Carnegie Mellon University, 2008, accessed December 15, 2020, accessed 20 December 2020, https://us-cert.cisa.gov/sites/default/files/publications/infosecuritybasics.pdf.

[81] Sara L. Zeigler, "Communications Decency Act of 1996," *The First Amendment Encyclopedia*, 2009, accessed December 20, 2020, https://www.mtsu.edu/first-amendment/article/1070/communications-decency-act-of-1996.

communications.[82] The regulation borrowed from previous regulations and court precedence to make criminal communicating indecent images over the Internet to children. Section 230 extends protections to Internet service and content providers providing immunity from liability and prosecution for content uploaded to their services by customers.[83] It also protects them from liability should they remove content they deem in violation of section 230. The content they or any of their users consider to be objectionable - regardless of whether the content is constitutionally protected speech - can be removed with little legal recourse; conversely, if these were government rather than private service providers, such would be an act of censorship.

There are those who want to repeal this Section outright, those that wish to modify it, and those that see no problem. The issue at hand is that the regulations make social media companies the arbiters over speech on their platforms, which even they have said should be further regulated.[84] The FCC and the Communications Decency Act were designed for controlling radio and television content broadcast by licensed stations. Neither was designed for monitoring or policing the billions of posts that make up social media content or the associated advertising markets and the revenue associated with the content. Additional oversight to protect election-integrity is being called for by Congressman Rodney Davis author of "Stopping Harmful Interference In Elections For A Lasting Democracy Act."[85] Neither the Intelligence community nor the DoD as currently authorized is capable of addressing the issues in the Information Domain; and the FCC, like other government cybersecurity entities, lacks the resources to address the problem.

---

[82] Zeigler, "Communications Decency Act of 1996."

[83] Ibid.

[84] Zuckerberg, "Four Ideas to Regulate the Internet."

[85] Davis Rodney, "H. Rept. 116-246 - Stopping Harmful Interference in Elections for a Lasting Democracy Act," Congress.gov, October 21, 2019, accessed 20 December 2020, https://www.Congress.gov/congressional-report/116th-Congress/house-report/246.

The associated regulatory framework within the US was not designed to protect the Information Domain from attack, but rather to control the application of information technologies found within other spheres of human activity. The need for a defense capability in the information environment has emerged in a manner similar to the need for cyber capability within DoD. Each military service previously had signals, information, and intelligence capabilities; however, as the cyber domain matured, the creation of new entities for the express purpose of acting in the cyber-domain became necessary—but the associated regulatory frameworks limit actions by those services within the US domestic information environment. Were the US to consider the Information Domain as an environment of action in need of regulation and military protection as it has emerged, actions to protect US sovereignty are understandable and supportable. Respect for civil liberties and the rule of law are not impediments to such action. The commercial aspects of the domain alone demonstrate a need of new defensive capabilities, including ability to act in the Information Domain below the level of armed conflict for regulatory, health and safety issues. Such a capability would also enable sharing of information and when necessary create a bridge over the divide between civil and military action.

Analysis

Supporting and defending the constitution is the first principle of US law and policy. In light of first amendment protections of speech and the press, there should be little wonder why the US has yet to identify a central government entity responsible for information operations. Though DoD possesses the most significant government capability for information operations, having established USCYBERCOM and the service cyber forces, the use of such capability domestically is illegal and a social taboo in the US. Additional capacity exists elsewhere within the US Military, primarily in units for civil affairs and psychological operations for the conduct of operations in either the cyber domain or information environment. As said, however, there are

severe constraints on DoD activity with regard to law enforcement and also for domestic actions in the Information Domain.

The National Defense Authorization Acts (NDAA) from 2017-2019 have expressly prohibited DoD from using appropriated funds for conducting domestic publicity or propaganda without the Secretary of Defense offering a plan to integrate its efforts with the State Department's Global Engagement Center.[86] The Global Engagement Center is an 80 person State Department organization established in the 2017 NDAA with the mission of to "lead, synchronize, and coordinate efforts of the Federal Government to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining United States national security interests."[87] Though DoD and the State Department have some clear roles and capabilities, the State Department is identified to lead counter propaganda and disinformation efforts. This task, however, represents a narrative and public relations activity rather than a defensive or warning capability. Other than current law enforcement entities with very limited authority, there is no preeminent organization for overall responsibility for safety, regulatory, or policing actions within the information environment/cyberspace domain in the US.

The US does have law enforcement organizations operating in the Information Domain to address cyber-crime and network or cyber-security requirements. The FBI and DHS are the two major players outside DoD and State Department; however, States and other localities have some capability as well. The US approach is distributed with different levels, authorities, and responsibilities, which is in keeping with the diffused power structures created under the Constitution in other fields of law. This design is meant to provide victims of crime places to

[86] John S. McCain National Defense Authorization Act for Fiscal Year 2019, H.R. 5515, 115th Cong., 2nd sess., January 3, 2018.

[87] National Defense Authorization Act for Fiscal Year 2017, Public Law 114-328, 114th Cong., 2nd sess., December 23, 2016.

report incidents; however, there is no "patrolling" of the area to identify or deter crimes. The US does not have centralized surveillance of telecommunications, like Russia or China. However, law enforcement at most levels is capable of conducting such surveillance. However, employment of capability is associated with wiretapping and has Fourth Amendment protections, which means operations are limited and require warrants as authorization for action.

Intelligence capabilities within both the FBI and the NSA are capable of monitoring and collecting such information from the Internet. Currently, they too are bound by strict legal processes in place to prevent potential exploitation of information on US citizens without a court-approved warrant. Indeed, where Russian and Chinese law requires Internet service providers to install surveillance equipment, in the US, such equipment is only found on networks physically operated by the government, resulting in the US government having to rely on the cooperation of private sector companies for reporting of any nefarious activity, or for them to have probable cause when they desire a warrant.

Public-private cooperation to address security is part of the US model. Citing growing cyberthreats to US infrastructure, in 2015 President Obama ordered the Director of National Intelligence to establish the Cyber Threat Intelligence Integration Center. This action was done under authorities established under the Intelligence Reform and Terrorism Prevention Act of 2004.[88] This integrated center provides intelligence concerning foreign cyber-threats and cyber-incidents impacting US national interests to US government centers responsible for cybersecurity and network defense. Cyber Threat Intelligence Integration Center also provides assistance to private sector partners to facilitate efforts to counter foreign cyber threats.[89] This organization

[88] Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458, 108th Cong., December 17, 2004.

[89] The White House, "Fact Sheet: Cyber Threat Intelligence Integration Center," Office of the Press Secretary, February 25, 2015, accessed 20 December 2020, https://obamawhitehouse.archives.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center.

represents another effort to coordinate actions by disparate government and private sector organizations reacting to threats within the cyberspace domain; it, however, does little to nothing concerning the information environment, especially since some of those threats may be from commercial entities themselves.

The concerns over foreign cyber-threats spawned changes to DoD forces, including expanded authorities and growing missions. In 2018 a panel of National Guard leaders discussed efforts to build and equip the guard as it took on expanding cybersecurity roles as part of the US military's cyber mission force. The panel highlighted challenges posed by new technologies and highlighted the essential operation that the Army conducts as the 24/7 security and operation of "our" networks.[90] This panel highlights an ongoing growth effort in the Guard to provide cyber protection to state and municipal networks.

The 2019 NDAA provided expanded authorities to DoD to act in the domain, including an authority to act against actions by Russia, China, Iran, or North Korea proportionally in response to actions in cyberspace against US national interests.[91] The NDAA, along with the reported authorities in National Security Presidential Directive 13,[92] has allowed USCYBERCOM to defend forward as it took on the mission to protect US elections in 2018 and 2020.[93] This expansion of mission was seen as part of the "norms-based" approach to securing the domain.

---

[90] SSG Michael Cardin, "Leaders Discuss Future of National Guard Cyber Warfare," *Guard News*, May 21, 2018, accessed 20 December 2020, https://www.nationalguard.mil/News/Article/1527175/leaders-discuss-future-of-national-guard-cyber-warfare/.

[91] John S. McCain National Defense Authorization Act for Fiscal Year 2019, H.R. 5515, 115th Cong., 2nd sess., January 3, 2018.

[92] Ellen Nakashima, "White House Authorizes 'Offensive Cyber Operations' to Deter Foreign Adversaries," *The Washington Post*, September 22, 2018, accessed 20 December 2020, https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html.

[93] Mark Pomerleau, "New Authorities Mean Lots of New Missions at Cyber Command," Fifth Domain, May 8, 2019, accessed 20 December 2020, https://www.fifthdomain.com/dod/cybercom/2019/05/08/new-authorities-mean-lots-of-new-missions-at-cyber-command/.

In 2011 the US published its International Strategy for Cyberspace, which defined the norms-based approach to international cooperation in cyberspace. It rests on five principles including: upholding fundamental freedoms, respect for property, valuing privacy, protection from crime, and the right of self-defense.[94] These principles are grounded in international agreements such as the UN Charter as well as fundamental rights identified in the US Constitution. In 2015 the UN Group of Government Experts published a report on recommendations to promote security and cooperation among nations, including a discussion of norms that are the current basis for US policy development.[95] Washington continues to push through bilateral, multilateral, and UN forums advocating this norms-based approach for behavior in the Information Domain. The US effort to frame cooperation has come under increasing scrutiny since it was published due in part to alternative techniques and exposure of US actions, which have been characterized as hypocritical. For example, in 2013 the revelation of US intelligence surveillance programs and cooperation with big tech firms by Edward Snowden arguably undermined the integrity of the US principles of "valuing privacy."[96]

The US claims the norms-based approach does not require a reinvention of international law. Further, it does not make existing international norms obsolete. In fact, the strategy explicitly states existing norms that guide state behavior, both in peace and war, apply to cyberspace. As the 2011 strategy said, "understanding that an important first step in such efforts is applying the broad expectations of peaceful and just interstate conduct to cyberspace."[97] Interestingly, none of the norms listed suggest the prohibition of policing common areas.

---

[94] President of the United States, *US International Strategy For Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: The Whitehouse, 2011).

[95] UN General Assembly, "Group of Governmental Experts," accessed December 15, 2020, accessed 20 December 2020, https://www.un.org/disarmament/group-of-governmental-experts/.

[96] Ellen Nakashima, "From Obscurity to Notoriety, Snowden Took an Unusual Path," *The Washington Post*, June 9, 2013, accessed 20 December 2020, https://www.washingtonpost.com/world/national-security/from-obscurity-to-notoriety-snowden-took-an-unusual-path/2013/06/09/dc2e4274-d15b-11e2-9f1a-1a7cdee20287_story.html.

[97] President of the United States, *US International Strategy For Cyberspace.*

There are fundamental linkages among the information environment, the cyber domain, national security, and individual liberty. The US norms-based approach would seek to include freedom of speech and expression as specific norms to be included as part of the approach. How the US further organizes and acts to protect its own national sovereignty and the rights of its citizens should recognize these linkages and guide its actions in establishing more coherent policies as the means to effect security and cooperation. A recent effort in this regard is the 2020 a congressionally sponsored review of cyberspace capability undertaken by the CSC, which reviewed current government cybersecurity efforts and made recommendations for changes to address shortcomings. The existing entity identified within the CSC report as a potential lead for cybersecurity is the Cybersecurity and Infrastructure Security Agency (CISA), currently an administrative office in the DHS. The CSC report recommends CISA be expanded to a full agency with authority to collaborate and coordinate with other government entities and private sector partners in matters of cybersecurity.

The CSC suggests the DoD conduct a force structure assessment including eight recommendations including the following: creation of a major program for training manning and equipping USCYBERCOM; expanding the reporting program within the US government for public disclosure of malware; changes to the delegation of Title 10 authorities; a reassessment of cyber rules of engagement and rules on the use of force; increased cooperation with allies and partners; defining of reporting metrics for effectiveness of cyber operations; the establishment of a cyber reserve; and cyber professors at the military professional development colleges.[98] Establishing CISA as a lead entity would enable DHS to respond to incidents against infrastructure and cooperate with the private sector, but only allows monitoring of government networks and not the environment in general. It would also enable DoD to create a capability for military responses to attacks and acting forward to identify threats outside the US as well as

[98] King and Gallagher, *United States of America Cyberspace Solarium Commission*, 117-118.

cooperating with allies and partners in this action. In short, CISA would operate domestically in the domain while USCYBERCOM is operating forward for Title 10 defense.

The US has multiple entities with the capability and authority to act in the Information Domain. These organizations, however, are each part of a parent organization, meaning their efforts in the Information Domain remain tethered to those parent entities' original mission sets. For example, while the US State Department has a counter-narrative capability in the Global Engagement Center, officials are hesitant to use such capability in order to avoid accusations of conducting information or influence operations risks undermining their diplomatic mission.

This tethering of capability to original missions is also present within US intelligence capability and the disparate number of law enforcement agencies currently monitoring and regulating pieces of the Information Domain. The original purposes, authorities, and mandates for each of these entities were designed for them to be able to conduct a core mission using the Information Domain, not to police the Information Domain itself. For example, as communications became more computer network-based in the 1980s to 1990s, US signals intelligence capability began focusing on the ability to garner intelligence from computer networks. A few decades later, USCYBERCOM was established from capabilities developed by the NSA, and the two arguably separate entities remain linked to this day.[99] Understanding that most government entities created their Information Domain capability to accomplish their original missions suggests there remains a need for a holistic Information Domain organization that adopted ways and means specifically to operate in the information environment and cyberspace; capabilities that emerged as an extension of those original missions into policing the information environment have proven insufficient. The emergent nature of the Information Domain as an environment in its own right has grown beyond the ability of government agencies

[99] James Di Pane, "Now Is Not the Right Time to Split NSA and CYBERCOM," *C4ISRNET*, December 29, 2020, accessed 29 December 2020, https://www.c4isrnet.com/opinion/2020/12/29/now-is-not-the-right-time-to-split-nsa-and-cybercom/.

to stretch their capabilities to defend. Some threats in the domain risk conflict escalation and the military lacks specific authorities to act domestically below the threshold of armed conflict. There is a need for capability in government for the administration of laws, enforcement of regulations, and monitoring of the Information Domain subject to US jurisdiction and sovereignty.

The CSC report recognizes the connection of the Information Domain just as Russia and China have, including a recommendation of including delegation of information warfare authorities to USCYBERCOM as appropriate.[100] If it is also accepted that the Information Domain is a global domain including commercial activity below the threshold of war, it seems logical that the US should have a capability to patrol and operate across that domestic/foreign divide. Such an entity capable of operating domestically under authorities for law enforcement/regulation could support a warning function while simultaneously cooperating with industry and other government entities for regulatory/law enforcement purposes. It would also be designed to integrate with DoD in the event of escalation. This is not to suggest the usurpation of authorities, but rather the creation of an entity with its own powers to enforce current law in the Information Domain as well as serve as a focal point for understanding law, technology, regulations, health, and safety in the Information Domain.

Such an entity and corresponding authorities are a missing element of the US approach to the Information Domain. The creation of an organization specifically mandated to regulate and monitor the Information Domain represents recognition of the nature of the Information Domain as a global commons. So, while the different elements of the US government currently represent some capability to defend their own government networks, to respond to reported property crime, and provide advice for network security, there remains a need for a holistic entity with authority to monitor, provide warning concerning threats, cooperate with industry, promulgate health and safety, secure liberty and US sovereignty to reduce the risk of conflict.

[100] King and Gallagher, *United States of America Cyberspace Solarium Commission*, 115.

Consider also the impact of emergent phenomena such as recent actions associated with social media companies where a corporation banned the account of the President of the United States in effect censoring him.[101] and whether resultant to such actions, as critics argue, that such activities possibly enable foreign threats. Additional issues in public health exist as medical professionals have identified possible increased health risks related to compulsive behavior among social media users.[102] Additionally social media companies have been accused of limiting access to markets in arguably in violation of equal opportunity statutes.[103] These argument indicate that the Information Domain has matured to a point where the capability to implement health and safety regulatory structures within the information environment and domain is clear.

Facebook is a good example: as of October 2020 it had approximately 2.7 billion individual user accounts.[104] Legally Facebook is a US Corporation, and its networks hosting and sharing the content of those 2.7 billion users is protected as if it were a single US person in their private residence. This means under current legal strictures any US law enforcement or intelligence agency requires a warrant for any investigation or law enforcement monitoring beyond the public-facing web page. But if the US population is about 325 million, each denizen would have to have eight separate Facebook accounts for it to be wholly American. This global nature suggests that Facebook and other social media sites represent less the US person in their parent organization, and more a global commons which is effectively subject to US jurisdiction

[101] Brian Fung, "Twitter Bans President Trump Permanently," *Cable News Network*, January 9, 2021, accessed 20 January 2021, https://www.cnn.com/2021/01/08/tech/trump-twitter-ban/index.html.

[102] McLean Hospital, "The Social Dilemma: Social Media and Your Mental Health," McLean Hospital, February 10, 2021, accessed 10 February 2021, https://www.mcleanhospital.org/essential/it-or-not-social-medias-affecting-your-mental-health.

[103] Mehreen Kasana, "YouTube Hit with Discrimination Lawsuit by Black Creators over Shady Profiling Tactics," *Input*, June 18, 2020, accessed 20 January 2021, https://www.inputmag.com/culture/group-of-black-content-creators-slam-youtube-with-lawsuit-for-alleged-discrimination.

[104] J. Clement, "Number of Monthly Active Facebook Users Worldwide as of the beginning of the 4th Quarter 2020," Statista, accessed November 4, 2020, https://www.statista.com/statistics/264810 /number-of-monthly-active-facebook-users-worldwide/.

and regulation. Considering how targeted Facebook advertisements were central to the identified national security threat of election interference in 2016, 2018, and 2020, it seems changes to oversight, and regulation of these global commons is in order. The ability to patrol and monitor such global commons, networks, and data centers where commerce is conducted, including the back-end layers for nefarious activity, is warranted. While USCYBERCOM has used its new authorities to defend forward, a form of long-range patrolling,[105] there remains a need for authorities to patrol and act in areas of the domestic Internet, in effect in patrolling in coastal waters.

Twitter offers another example of the need for regulation within the domain outside traditional military activity. In October of 2020, the *New York Post's* Twitter account was suspended for publication of a politically contentious story. This action hid the story from anyone using the Twitter platform to identify news stories and to discuss them. This deliberate blocking of content, even if done by the hosting platform, represents the exact same sort of election interference deemed a national security threat in 2016.[106] Lacking a regulatory entity to protect against violation of free speech or to take action for malign influence/misinformation, social media companies themselves are determining which stories are being published. In this they are protected by FCC Regulation 230 while taking action in a manner identified as a national security threat when taken by foreign powers.

The 2016 use of social media company advertisements and platforms by foreign powers as vehicles for their influence operations resulted in actions to secure future elections from

[105] Mark Pomerleau, "Here's How Cyber Command Is Using 'Defend Forward'," Fifth Domain, November 12, 2019, accessed 20 January 2021, https://www.fifthdomain.com/smr/cybercon/2019/11/12/heres-how-cyber-command-is-using-defend-forward/.

[106] Todd Spangler, "Twitter Unblocks Account of New York Post, Which Claims Victory in Standoff Over Biden Stories," *Variety*, November 1, 2020, accessed 20 January 2021, https://variety.com/2020/digital/news/twitter-unblocks-new-york-post-hunter-biden-hacked-materials-1234820449.

interference, but little substantive action to regulate the domain to actually prevent it.[107] This inconsistent action by the US Government has resulted in widespread mistrust of both the government and media companies. The Senate held a hearing concerning the 2016 incident and others; however, only anecdotal evidence was available as there is no government entity with express authority to monitor and regulate the domain that might gather evidence for review. Providing oversight and central point of contact to lodge complaints and or to cooperate with as a government regulatory and enforcement service is a means to restore trust both internally to the US and externally with other nations.

Recommendation and Conclusion

The Information Domain as discussed represents an emergent operational environment as discussed and represented doctrinally as the Information Environment in DoD Joint publications.[108] Visualizing the change this emergence represents is a good starting point to formulate an organizational approach. The original Information Environment is shown in Figure 3.

[107] Clapper, *Assessing Russian Activities and Intentions in Recent US Elections*.

[108] Joint Staff, JP 3-13, *Information Operations.*

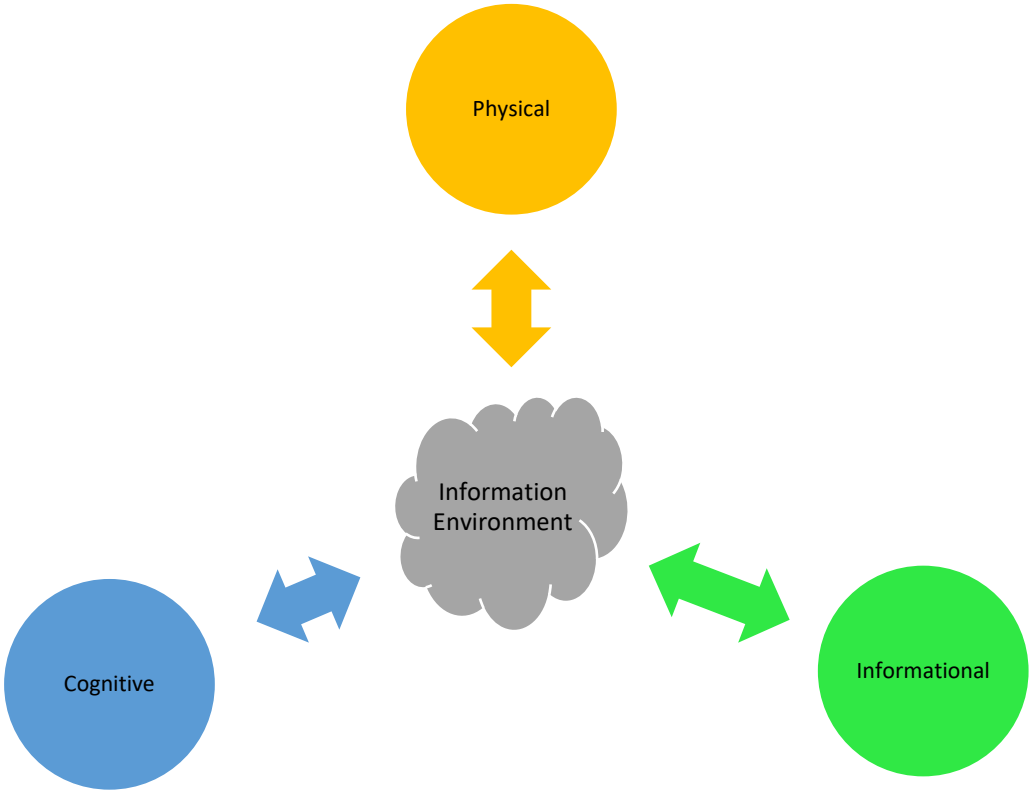

Figure 3. Historical Information Environment Visualized. Created by author to visually represent the origins of Information Domain. *Source* created by author.

Prior to the Internet, threats were considered manageable because of the size, scope, and scale of the information environment. In that era the physical dimension was telephone, radio, and television, and the informational print media, books, mail. Most emergent phenomenon within this era came from the cognitive and as discussed, the stove-piped regulatory environment emerged to manage specific physical aspects or elements of the environment. Licensing of radio and television stations and the communications decency act to restrict salacious content broadcast to the general public to protect children are examples from this approach. There was also criminal law associated with fraud and counterfeiting as well as copyright law to protect intellectual property. The key point in this construct is that each of these spheres of activity are within the Information Domain but remain almost entirely inside its original physical sphere with little to no overlap.

Figure 4, however, demonstrates the emergent aspect that is the Information Domain as it presents in the globally interconnected world today.

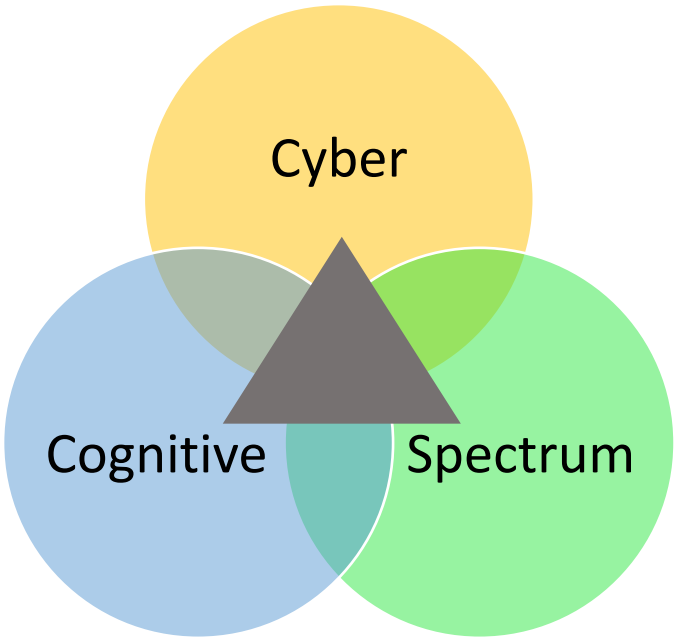

Figure 4. The Emergent Information Domain Visualized. Created by author to visually represent the current state of the Information Domain. *Source* created by author.

The amount of information generated globally, and that information's inter-connectivity has enabled collaboration, data sharing, commerce, innovation, and creation of social groups which were previously impossible. This represents an overlapping of cognitive, physical, and informational aspects of the original information environment which results in the emergent area the Information Domain. It is in this area of rapid convergence where threats begin to emerge.

Considering this convergence creating the Information Domain, what might be done by the US to address overlaps in regulatory, security, public health, and civil liberties issues? A new entity responsible for the emergent Information Domain would be preferable to continued simple extension of the authorities of existing organizations. There is already an effort to elevate existing entities in DHS to the level of a new agency as a focal point for its cyber security. The CSC report recommends this elevation and empowerment of CISA to a full agency to create a new

focal point for coordination of cybersecurity and physical infrastructure protection.[109] The Solarium suggests many other efforts to strengthen existing cyber security entities to reinforce or expand their current capabilities against cyberthreats. This is an admirable idea for the cyberspace portion of the information environment. However, this action as well as recommended changes to military within it still ignores the emergent Information Domain. Consider the Army's reorganizing of its Cyber Center of Excellence to include information and electronic warfare.[110]

Perhaps a new agency should also be considered to manage the convergent aspects of the Information Domain as shown by the grey triangle in Figure 4. In order to be effective as a focal point such an entity would require authority not just for cyberspace, but for existing laws and regulations related to the Information Domain. To accomplish this, it would be prudent to consider a similar regulatory framework to Title 14 of the US Code which establishes the US Coast Guard. Under Title 14 the Coast Guard is empowered to enforce or assist in the enforcement of all applicable Federal laws in its domain. Additionally, it can engage surveillance or interdiction to enforce or assist in the enforcement of and to administer laws. It is charged with the promulgation and enforcement of regulations in its domain. Finally, Title 14 empowers the Coast Guard to enable national defense and develop or foster international agreements for the maritime domain.[111]

---

[109] King and Gallagher, *United States of America Cyberspace Solarium Commission*, 39-41.

[110] As Army Cyber Command looks to focus on the information warfare environment, the Army's Cyber Center of Excellence in Georgia has started training cyber and electronic warfare personnel on the specifics of information operations. "We've been thinking about it for many months now, about how we're going to integrate what is going on in information operations with what's going on with both running, defending and doing cyberspace operations and electronic warfare," Col. Paul Craft, commandant of the cyber school at Fort Gordon, told reporters during a phone call January 15, 2020. Mark Pomerleau, "The Army's Cyber School Now Teaches Information Operations," Fifth Domain, January 17, 2020, accessed 20 January 2021, https://www.fifthdomain.com/dod/army/2020/01/16/the-armys-cyber-school-now-teaches-information-operations/.

[111] Cornell Law School, "US Code: Title 14-Coast Guard," Cornell University, accessed December 15, 2020, https://www.law.cornell.edu/uscode/text/14.

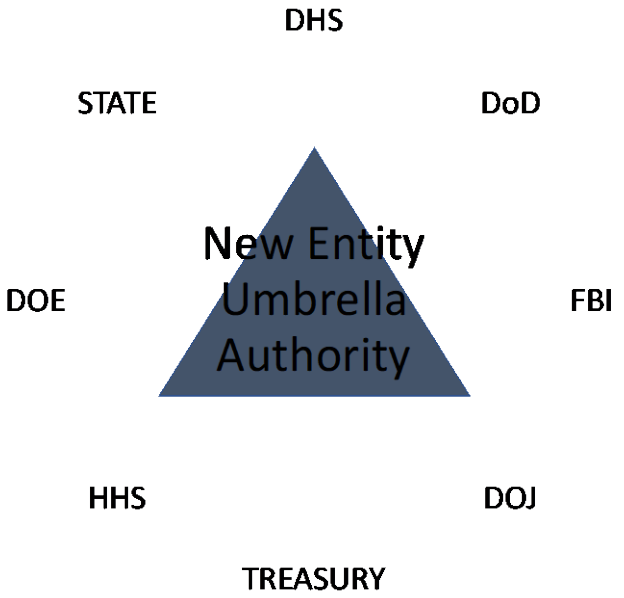

Figure 5. The New Entity Concept Visualized. Created by author to visually represent a new regulatory entity for the Information Domain. *Source* created by author.

Creating an entity for the Information Domain with similar mandates would provide a focal point for the Information Domain (See Figure 5). For example in such a construct, Health and Human Services would study the medical aspects resultant from use of social media, including increased depression and dwindling attention spans.[112] Medical professionals in HHS, however, would be only a part of regulatory response. The central entity for the Information Domain, capable of understanding and coordinating other aspects of the law pertaining to restriction of content would be part as well. Including, once rules are in place, employing technical experts to monitor activity of online companies and ensure compliance. Such an agency could be composed of a core of employees directly assigned to it as well as detailed employees, to

[112] Elina Mir, Caroline Novas, and Meg Seymour, "Social Media and Adolescents' and Young Adults' Mental Health" (National Center for Health Research, August 21, 2020), accessed 20 January 2021, https://www.center4research.org/social-media-affects-mental-health/.

include military members, from other agencies to enable collaboration as envisioned in the SCS report.

The general legal authorities of such an entity modeled after Title 14 as an umbrella for all federal laws and regulations would best extend to anyone working directly for or detailed to the entity. However, to avoid interagency competition and redundancy issues, it might be preferable to have law-enforcement and arrest powers retained by the originating agency. This would allow the new entity to focus on monitoring the environment and coordinating and promulgating regulations to ensure national security and civil liberties. This arrangement could also bridge the gap for activities below the threshold of war and DoD activities covered under Title 10 and Title 50. Detailed military members to the new agency would be enabled to monitor and understand impacts of activities domestically to fill in gaps where foreign threat actors are involved. Currently, the Intelligence Community acts as a sort of focal point for such collaboration. This arrangement tends to leave industry at a disadvantage due to security clearance issues. However, having a new entity with general Internet monitoring as well as intelligence authorities would strengthen the whole of nation paradigm as envisioned in the CSC report.[113] Such an entity with a detail enabled organization would create a smooth transition and interaction for inter-agency activities protecting near and DoD activities defending forward in cyberspace and elsewhere in the Information Domain as envisioned by DoD.

The entity would need an organic Intelligence Capability for the Information Domain and would collaborate with the rest of the community. It would need specific intelligence collection authorities to enable monitoring of the domestic Information Domain. Such authorities however would be designed with an understanding of the regulatory environment as well as the technical nature of the information infrastructures and data. Coupling this with specific direction to protect

[113] King and Gallagher, *United States of America Cyberspace Solarium Commission*, 23.

US citizens civil liberties as a primary goal of the new entity as well as designing and including specific oversight and transparency rules would ensure the protection of the people.

Such an entity complements the actions of the CSC report recommendations and may represent a broader way to achieve national security for both cyberspace and the broader Information Domain as described. Moreover, a regulatory entity for the Information Domain would be a neutral arbiter for the people as the government should be. With civil liberties as a guide, it would be charged to ensure that within the Information Domain subject to US jurisdiction individual liberty and freedom of speech are the norm, rather than outsourced political censorship. In doing this, we secure the blessings of liberty, to ourselves and our posterity.

Bibliography

Allen, Gavin, ed. “Lese-Majeste Explained: How Thailand Forbids Insult of Its Royalty.” *BBC News*, October 6, 2017. Accessed 28 February 2021, https://www.bbc.com/news/world-asia-29628191.

Atha, Katherine, Jason Callahan, John Chen, Jessica Drun, Ed Francis, Kieran Green, Dr. Brian Lafferty, Joe McReynolds, Dr. James Mulvenon, Benjamin Rosen, and Emily Walz. “China’s Smart Cities Development.” Research Report prepared on behalf of the US-China Economic and Security Review Commission, SOS International, Vienna, VA, 2020.

Bambauer, Derek E. “How Section 230 Reform Endangers Internet Free Speech.” Brookings, July 16, 2020. Accessed 28 February 2021, https://www.brookings.edu/techstream/how-section-230-reform-endangers-internet-free-speech/.

Basu, Soutrik, Joost Jongerden, and Guido Ruivenkamp. “Development of the Drought Tolerant Variety Sahbhagi Dhan: Exploring the Concepts Commons and Community Building.” *International Journal of the Commons* 11, no. 1 (March 2017): 144-170. Accessed 28 February 2021, https://www.thecommonsjournal.org/article/10.18352/ijc.673/.

Berger, Peter L., and Thomas Luckmann. *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*. New York: Anchor Books, 1967.

Blackhat. Directed by Michael Mann. Internet Movie Database, January 14, 2015, 2 hr., 13 min. Accessed 28 February 2021, https://www.imdb.com/title/tt2717822/?ref_=fn_al_tt_1.

Blunden, Bill, and Violet Cheung. *Behold a Pale Farce: Cyberwar, Threat Inflation, and the Malware Industrial Complex*. Walterville, OR: Trine Day, 2014.

Browne, M. Neil., and Stuart M. Keeley. *Asking the Right Questions: A Guide to Critical Thinking*. Upper Saddle River, NJ: Pearson/Prentice Hall, 2007.

Cadell, Cate, and Pei Li. “Tea and Tiananmen: Inside China’s New Censorship Machine.” *Reuters*, September 29, 2017. Accessed 28 February 2021, https://www.reuters.com/article/china-Congress-censorship/tea-and-tiananmen-inside-chinas-new-censorship-machine-idUSL4N1LW25C.

Campbell, Charlie, and Cheng Du. “How China Is Using Big Data to Create a Social Credit Score.” *Time Magazine*, August 14, 2019. Accessed 28 February 2021, https://time.com/collection/davos-2019/5502592/china-social-credit-score/.

Cardin, SSG Michael. “Leaders Discuss Future of National Guard Cyber Warfare.” *Guard News*, May 21, 2018. Accessed 28 February 2021, https://www.nationalguard.mil/News/Article/1527175/leaders-discuss-future-of-national-guard-cyber-warfare/.

Cassin, René. “Universal Declaration of Human Rights.” United Nations General Assembly, December 10, 1948. Accessed 28 February 2021, https://www.un.org/en/universal-declaration-human-rights/.

CCD COE. “About Us.” CCD COE. Accessed December 20, 2020. Accessed 28 February 2021, https://ccdcoe.org/about-us/.

Childress, Sarah. “Bradley Manning Sentenced to 35 Years for WikiLeaks.” *Public Broadcasting Service*, August 21, 2013. Accessed 28 February 2021, https://www.pbs.org/wgbh/frontline/article/bradley-manning-sentenced-to-35-years-for-wikileaks/.

Clapper, James. ICA 2017-01, *Assessing Russian Activities and Intentions in Recent US Elections.* Washington, DC: National Intelligence Council, 2017.

Clausewitz, Carl Von. *On War*. Edited and Translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1984.

Clement, J. “Number of Monthly Active Facebook Users Worldwide as of the beginning of the 4th Quarter 2020.” Statista. Accessed November 4, 2020, https://www.statista.com /statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

Corbett, Julian S. *Some Principles of Maritime Strategy*. New York: Create Space, 2018.

Cornell Law School. “US Code: Title 14-Coast Guard.” Cornell University. Accessed December 15, 2020, https://www.law.cornell.edu/uscode/text/14.

Creemers, Rogier, Paul Triolo, and Graham Webster. “Translation: Cybersecurity Law of the People’s Republic of China (Effective June 1, 2017).” New America, June 29, 2018. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

Cybersecurity and Infrastructure Security Agency. “Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA).” Cybersecurity and Infrastructure Agency, January 5, 2021. Accessed 28 February 2021, https://www.cisa.gov /news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure.

Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation. “Internet Crime Complaint Center (IC3): False Claims of Hacked Voter Information Likely Intended to Cast Doubt on Legitimacy of US Elections.” Internet Crime Complaint Center (IC3), September 28, 2020. Accessed 28 February 2021, https://www.ic3.gov/Media/Y2020/PSA200928.

Davis, Rodney. “H. Rept. 116-246 - Stopping Harmful Interference in Elections for a Lasting Democracy Act.” Congress.gov, October 21, 2019. Accessed 28 February 2021, https://www.Congress.gov/congressional-report/116th-Congress/house-report/246.

Dewey, Caitlin. “Russia Just Made a Ton of Internet Memes Illegal.” *The Washington Post*, April 10, 2015. Accessed 28 February 2021, https://www.washingtonpost.com/news/the-intersect/wp/2015/04/10/russia-just-made-a-ton-of-internet-memes-illegal/.

Drogin, Bob. *Curveball: Spies, Lies, and the Man behind Them: The Real Reason America Went to War in Iraq*. London: Ebury, 2008.

Epifanova, Alena. "Deciphering Russia's 'Sovereign Internet Law:' Tightening Control and Accelerating the Splinternet." *DGAP Analysis*, no. 2 (January 2020): 1-11.

Esper, Mark T. "The United States Builds Relationships..." US Secretary of Defense, Facebook, September 7, 2020. Accessed September 7, 2020. Accessed 28 February 2021, https://www.facebook.com/SecDef/photos/a.140591818639727 4/2747519962237083.

Federal Aviation Administration. "FAADroneZone." US Department of Transportation, December 28, 2020. Accessed 28 February 2021, https://faadronezone.faa.gov/#/.

FireEye. "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor." *FireEye* (blog), December 13, 2020. Accessed 28 February 2021, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html.

Fung, Brian. "Twitter Bans President Trump Permanently." *Cable News Network*, January 9, 2021. Accessed 28 February 2021, https://www.cnn.com/2021/01/08/tech/trump-twitter-ban/index.html.

Gaddis, John Lewis. *The Landscape of History: How Historians Map the Past*. New York: Oxford University Press, 2002.

Gat, Azar. *A History of Military Thought: from the Enlightenment to the Cold War*. New York: Oxford University Press, 2001.

GCN Staff. "National Guard on Hand for Election Cybersecurity." GCN, October 22, 2020. Accessed December 20, 2020. Accessed 28 February 2021, https://gcn.com/articles/2020/10/22/national-guard-cyber-election-defense.aspx.

Gutterman, Roy S. "Sedition Laws and Free Speech." Jurist, Legal News and Commentary, May 14, 2015. Accessed 28 February 2021, https://www.jurist.org/commentary/2015/05/roy-gutterman-sedition-laws/.

Haidt, Jonathan. *The Righteous Mind: Why Good People Are Divided by Politics and Religion*. New York: Vintage Books, 2013.

Hennigan, W. J. "Pentagon Establishes No Drone Zone for Recreational UAVs." Government Technology, April 1, 2016. Accessed 28 February 2021, https://www.govtech.com/public-safety/Pentagon-Establishes-No-Drone-Zone-for-Recreational-UAVs.html.

Ilhan, Bekir. *China's Evolving Military Doctrine After The Cold War*. Washington, DC: SETA, 2020. Accessed 28 February 2021, https://setav.org/en/assets/uploads/2020/02/A56En.pdf.

Intel.gov. "How The IC Works." Intel.gov. Accessed December 15, 2020. Accessed 28 February 2021, https://www.intelligence.gov/how-the-ic-works#oversight.

Ismailov, Famil. “Russia Enacts ‘Draconian’ Law for Bloggers and Online Media.” *BBC News*, July 31, 2014. Accessed 28 February 2021, https://www.bbc.com/news/technology-28583669.

Isserson, G. S. *The Evolution of Operational Art*. Translated by Bruce Menning. Fort Leavenworth, KS: Combat Studies Institute Press, 2013.

Jibilian, Isabella. “Here’s a Simple Explanation of How the Massive SolarWinds Hack Happened and Why It’s Such a Big Deal.” *Business Insider*, December 24, 2020. Accessed 28 February 2021, https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.

Kahneman, Daniel. *Thinking, Fast and Slow*. New York: Farrar, Straus, and Giroux, 2015.

Kasana, Mehreen. “YouTube Hit with Discrimination Lawsuit by Black Creators over Shady Profiling Tactics.” *Input*, June 18, 2020. https://www.inputmag.com/culture/group-of-black-content-creators-slam-youtube-with-lawsuit-for-alleged-discrimination.

King, Angus, and Mike Gallagher. *United States of America Cyberspace Solarium Commission.* Washington, DC: Government Publishing Office, 2020.

Laperruque, Jake. “The History and Future of Mass Metadata Surveillance.” Project On Government Oversight, June 11, 2019. Accessed 28 February 2021, https://www.pogo.org/analysis/2019/06/the-history-and-future-of-mass-metadata-surveillance/.

Lee, Douglas E. “Seditious Libel.” *The First Amendment Encyclopedia*, October 2016. Accessed December 15, 2020. Accessed 28 February 2021, https://www.mtsu.edu/first-amendment/article/1017/seditious-libel#:~:text=Congress%20criminalized%20seditious%20libel%20in%201798&text=In%201798%20Congress%20passed%20four,the%20government%20or%20its%20officials.

Lewis, James Andrew. “Reference Note on Russian Communications Surveillance.” Center for Strategic and International Studies, April 18, 2014. Accessed 28 February 2021, https://www.csis.org/analysis /reference-note-russian-communications-surveillance.

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

Maclean, Norman. *Young Men and Fire*. Chicago: University of Chicago Press, 1993.

Mahan, Alfred Thayer. *Influence of Sea Power upon History, 1660-1783 Volume 27*. TheClassics.US, 2013.

McLean Hospital. “The Social Dilemma: Social Media and Your Mental Health.” McLean Hospital, February 10, 2021. Accessed 28 February 2021, https://www.mcleanhospital.org/essential/it-or-not-social-medias-affecting-your-mental-health.

Ministry of Defense of the Russian Federation. "Russian Federation Armed Forces' Information Space Activities Concept." Ministry of Defence, 2016. Accessed December 15, 2020. https://eng.mil.ru/en/science/publications/more.htm?id=10845074%40cmsArticle.

Mir, Elina, Caroline Novas, and Meg Seymour. "Social Media and Adolescents' and Young Adults' Mental Health." National Center for Health Research, August 21, 2020. https://www.center4research.org/social-media-affects-mental-health/.

Morris, Margaret, and Gary Bennett. "Edward Snowden and the Defence of Privacy." *The Guardian*, October 20, 2019. Accessed 28 February 2021, https://www.theguardian.com/world/2019/oct/20/edward-snowden-and-the-defence-of-privacy.

Motta, Dan. "For Your Eyes Only: The Soviet Union and The Photocopier." Cobb Technologies, August 9, 2018. Accessed 28 February 2021, https://discover.cobbtechnologies.com/blog/the-soviet-union-and-the-photocopier.

Nakashima, Ellen. "From Obscurity to Notoriety, Snowden Took an Unusual Path." *The Washington Post*, June 9, 2013. Accessed 28 February 2021, https://www.washingtonpost.com/world/national-security/from-obscurity-to-notoriety-snowden-took-an-unusual-path/2013/06/09/dc2e4274-d15b-11e2-9f1a-1a7cdee20287_story.html.

———. "White House Authorizes 'Offensive Cyber Operations' to Deter Foreign Adversaries." *The Washington Post*, September 22, 2018. Accessed 28 February 2021, https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html.

———. "US Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms." *The Washington Post*, February 27, 2019. Accessed 28 February 2021, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

Navarria, Giovanni. "How the Internet Was Born: From the ARPANET to the Internet. The Conversation, November 2, 2016. Accessed 28 February 2021, https://theconversation.com/how-the-internet-was-born-from-the-arpanet-to-the-internet-68072.

Nikiforov, N. "Приказ Минкомсвязи Об Утверждении Правил Применения Оборудования Систем Коммутации, Включая Программное Обеспечение, Обеспечивающего Выполнение Установленных Действий При Проведении Оперативно-Розыскных Мероприятий [Order of the Ministry of Telecom and Mass Communications Concerning the Approval of the Regulations for the Use of Equipment for Switching Systems, Including Software, for the Implementation of the Specified Actions during Operative Investigative Activities]." Российская газета [Russian Gazette], July 18, 2014. Accessed 28 February 2021, https://rg.ru/2014/07/18/kommutacia-dok.html.

O'Brien, Danny. "China's Global Reach: Surveillance and Censorship Beyond the Great Firewall." Electronic Frontier Foundation, October 10, 2019. Accessed 28 February 2021, https://www.eff.org /deeplinks/2019/10/chinas-global-reach-surveillance-and-censorship-beyond-great-firewall.

Pane, James Di. "Now Is Not the Right Time to Split NSA and CYBERCOM." *C4ISRNET*, December 29, 2020. Accessed 28 February 2021, https://www.c4isrnet.com/opinion/2020/12/29/now-is-not-the-right-time-to-split-nsa-and-cybercom/.

Parks, Michael. "Soviets Free the Dreaded Photocopier." *Los Angeles Times*, October 5, 1989. Accessed 28 February 2021, https://www.latimes.com/archives/la-xpm-1989-10-05-mn-913-story.html.

Pesante, Linda. "Introduction to Information Security." Carnegie Mellon University, 2008. Accessed 28 February 2021, https://us-cert.cisa.gov/sites/default/files /publications/infosecuritybasics.pdf.

Phillips, James S. "The Rights of Indigenous Peoples under International Law." *Global Bioethics* 26, no. 2 (2015): 120–27. doi:10.1080/11287462.2015.1036514.

Pomerleau, Mark. "Here's How Cyber Command Is Using 'Defend Forward'." Fifth Domain, November 12, 2019. Accessed 28 February 2021, https://www.fifthdomain.com/smr/cybercon/2019/11/12/heres-how-cyber-command-is-using-defend-forward/.

———. "New Authorities Mean Lots of New Missions at Cyber Command." Fifth Domain, May 8, 2019. Accessed 28 February 2021, https://www.fifthdomain.com/dod/cybercom/2019/05/08/new-authorities-mean-lots-of-new-missions-at-cyber-command/.

———. "The Army's Cyber School Now Teaches Information Operations." Fifth Domain, January 17, 2020. Accessed 28 February 2021, https://www.fifthdomain.com/dod/army/2020/01/16/the-armys-cyber-school-now-teaches-information-operations/.

President of the United States. *US International Strategy For Cyberspace: Prosperity, Security, and Openness in a Networked World.* Washington, DC: The Whitehouse, 2011.

Putin, Vladimir. "Doctrine of Information Security of the Russian Federation." Ministry of Defense, December 5, 2016. Accessed 28 February 2021, https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.

———. "Military Doctrine of the Russian Federation." Diplomacy Online, December 25, 2014. Accessed 28 February 2021, https://rusemb.org.uk/press/2029.

———. "Военная Доктрина Российской Федерации [Military Doctrine of the Russian Federation]." Президент России [President of the Russian Federation], February 5, 2010. Accessed December 20, 2020. http://kremlin.ru/supplement/461.

———. “Приказ Минкомсвязи Об Утверждении Правил Применения Оборудования Систем Коммутации, Включая Программное Обеспечение, Обеспечивающего Выполнение Установленных Действий При Проведении Оперативно-Розыскных Мероприятий [Order of the Ministry of Telecom and Mass Communications Concerning the Approval of the Regulations for the Use of Equipment for Switching Systems, Including Software, for the Implementation of the Specified Actions during Operative Investigative Activities].” Российская газета [Russian Gazette], July 18, 2014. Accessed December 20, 2020. https://rg.ru/2014/07/18/kommutacia-dok.html.

———. “Russian Federation Armed Forces’ Information Space Activities Concept.” Ministry of Defence of the Russian Federation. Accessed December 15, 2020. https://eng.mil.ru/en/science/publications/more.htm?id=10845074%40cmsArticle.

———. “Основы Государственной Политики Российской Федерации в Области Международной Информационной Безопасности На Период До 2020 Года [The Information Security Policy of the Russian Federation for the Period up to 2020].” Совет Безопасности Российской Федерации [Security Council of the Russian Federation], July 24, 2013. Accessed 28 February 2021, http://www.scrf.gov.ru/security/information/document114/.

Ragosta, John A. “The Information Revolution--Culture and Sovereignty--a US Perspective.” *Canada-United States Law Journal* 24 (January1998.): 155-163. Accessed 28 February 2021, http://search.ebscohost.com.lumen.cgsccarl.com/login.aspx?direct=true&db=lgh&AN=1774434&site=ehost-live&scope=site.

Random House Websters Unabridged Dictionary. “Definition of Freedom.” New York: Random House, 2005. Accessed 28 February 2021, https://doi.org/23 February 2019.

Rempfer, Kyle. “Army Cyber Lobbies for Name Change This Year, as Information Warfare Grows in Importance.” *Army Times*, October 16, 2019. Accessed 28 February 2021, https://www.armytimes.com/news/your-army/2019/10/16/ausa-army-cyber-lobbies-for-name-change-this-year-as-information-warfare-grows-in-importance/.

Rid, Thomas. *Cyber War Will Not Take Place*. Oxford, UK: Oxford University Press, 2013.

Rogers, Admiral Michael, Director NSA/Commander USCYBERCOM. “Hearing of the House (Select) Intelligence Committee Subject: “Cybersecurity Threats: The Way Forward.” National Security Agency Central Security Service, November 20, 2014. Accessed 28 February 2021, https://www.nsa.gov/news-features/speeches-testimonies/Article/1620360/hearing-of-the-house-select-intelligence-committee-subject-cybersecurity-threat/.

Rogulin, Dimitriy. “Russia’s National Guard Rejects Media Reports about Establishing Cyber Intelligence.” TASS, March 16, 2017. Accessed 28 February 2021, https://tass.com/politics/935846.

Roser, Max, Hannah Ritchie, and Esteban Ortiz-Ospina. “Internet.” Our WorldinData.org, July 14, 2017. Accessed 28 February 2021, https://ourworldindata.org/internet.

Savage, Charlie. “N.S.A. Triples Collection of Data From US Phone Companies.” *The New York Times*, May 4, 2018. Accessed 28 February 2021, https://www.nytimes.com/2018/05/04/us/politics/nsa-surveillance-2017-annual-report.html.

Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge: Cambridge University Press, 2016.

Schmitt, Michael N., and Liis Vihul. “Respect for Sovereignty in Cyberspace.” *Texas Law Review* 95 (2017): 1639–70.

Select Committee on Intelligence. “Report of the Select Committee on Intelligence on the US Intelligence Community’s Prewar Intelligence Assessments on Iraq.” July 2004. Accessed December 20, 2020. Accessed 28 February 2021, https://www.Congress.gov/108/crpt/srpt301/CRPT-108srpt301.pdf.

Shanker, Thom. “Cyberwar Nominee Sees Gaps in Law.” *The New York Times*, April 14, 2010. Accessed 28 February 2021, https://www.nytimes.com/2010/04/15/world/15military.html.

Sharikov, Pasha. “Understanding the Russian Approach to Information Security.” *European Leadership Network*, January 16, 2018. Accessed 28 February 2021, https://www.europeanleadershipnetwork.org/commentary/understanding-the-russian-approach-to-information-security/.

Shenon, Philip. “House Passes Bill to Overhaul US Intelligence System.” *The New York Times*, December 7, 2004. Accessed December 20, 2020. Accessed 28 February 2021, https://www.nytimes.com/2004/12/07/politics/house-passes-bill-to-overhaul-us-intelligence-system.html.

Sheppard, Felicity. “The Internet over the Past 20 Years.” *ABC News Australia*, May 27, 2014. Accessed December 20, 2020. https://www.abc.net.au/news/2014-05-25/internet-changes-over-20-years/5470442?nw=0.

Smith, Scott. “Roles and Responsibilities for Defending the Nation from Cyber Attack.” Statement before the Senate Armed Services Committee, October 19, 2017. Accessed 28 February 2021, https://www.fbi.gov/news/testimony/cyber-roles-and-responsibilities.

Soldatov, Andre, and Irina Borogan. *The Red Web: The Struggle Between Russia’s Digital Dictators and the New Online Revolutionaries*. New York: Perseus Books Group, 2015.

Spangler, Todd. “Twitter Unblocks Account of New York Post, Which Claims Victory in Standoff Over Biden Stories.” *Variety*, November 1, 2020. Accessed December 20, 2020. https://variety.com/2020/digital/news/twitter-unblocks-new-york-post-hunter-biden-hacked-materials-1234820449/.

Sparks, Jared, ed. *The Works of Benjamin Franklin*, Vol II. London: Benjamin Franklin Stevens, 1882.

Stoll, Clifford. *The Cuckoo's Egg: inside the World of Computer Espionage*. New York: Doubleday, 1989.

Sukhankin, Sergey. "Russian National Guard: A New Oprichnina, 'Cyber Police' or Something Else?" The Jamestown Foundation, March 21, 2017. Accessed 28 February 2021, https://jamestown.org/program/russian-national-guard-new-oprichnina-cyber-police-something-else-2/.

Thailand Lawyer. "Thailand Law Library." Thailand Law Library RSS. Accessed December 15, 2020. Accessed 28 February 2021, https://library.siam-legal.com/thai-law/criminal-code-royal-family-sections-107-112/.

The State Council Information Office of the People's Republic of China. *China's Military Strategy*. Beijing, 2015. Jamestown.org. Accessed September 15, 2020. Accessed 28 February 2021, https://jamestown.org/wp-content/uploads/2016/07/China%E2%80%99s-Military-Strategy-2015.pdf.

The White House. "Fact Sheet: Cyber Threat Intelligence Integration Center." Office of the Press Secretary, February 25, 2015. Accessed 28 February 2021, https://obamawhitehouse.archives.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center.

Thompson, Kevin. "Statement of Changes in Beneficial Ownership." United States Securities and Exchange Commission, December 14, 2020. File Number 001-38711. Accessed December 14, 2020, https://www.sec.gov.

Tkacheva, Olesya, Lowell H. Schwartz, Martin C. Libicki, Julie E. Taylor, Jeffrey Martini, and Caroline Baxter. *Internet Freedom and Political Space*. Santa Monica, CA: RAND Corporation, 2013.

UN General Assembly. "Group of Governmental Experts." Accessed December 15, 2020. Accessed 28 February 2021, https://www.un.org/disarmament/group-of-governmental-experts/.

US Congress. "S.272 - High-Performance Computing Act of 1991." Congress.gov, December 9, 1991. Accessed 28 February 2021, https://www.Congress.gov/bill/102nd-Congress/senate-bill/272.

———. "US Code Index." Office of Law Revision Counsel. Accessed February 1, 2021. https://uscode.house.gov/browse.xhtml.

US Cyber Command. "US Cyber Command History." US CYBERCOM. Accessed February 9, 2021. https://www.cybercom.mil/About/History/.

US Department of Defense. Joint Staff. Joint Publication (JP) 3-0, *Joint Operations*. Washington, DC: Government Publishing Office, 2018.

———. Joint Staff. Joint Publication (JP) 3-07, *Joint Doctrine for Military Operations Other Than War*. Washington, DC: Government Printing Office, 1995.

———. Joint Staff. Joint Publication (JP) 3-12, *Cyberspace Operations*. Washington, DC: Government Publishing Office, 2018.

———. Joint Staff. Joint Publication (JP) 3-13, *Information Operations*. Washington, DC: Government Printing Office, 2014.

———. Joint Staff. Joint Publication (JP) 3-14, *Space Operations*. Washington, DC: Government Publishing Office, 2018.

———. Joint Staff. Joint Publication (JP) 3-30, *Joint Air Operations*. Washington, DC: Government Publishing Office, 2019.

———. Joint Staff. Joint Publication (JP) 3-31, *Joint Land Operations*. Washington, DC: Government Publishing Office, 2019.

———. Joint Staff. Joint Publication (JP) 3-32, *Joint Maritime Operations*. Washington, DC: Government Publishing Office, 2018.

———. *National Defense Strategy*. Washington, DC: Government Publishing Office, 2018.

Wang, Maya. "China's Chilling 'Social Credit' Blacklist." *Human Rights Watch*, October 28, 2020. Accessed December 20, 2020. Accessed 28 February 2021, https://www.hrw.org/news/2017/12/12/chinas-chilling-social-credit-blacklist#.

Washington, George. "The Constitution of the United States: A Transcription." National Archives and Records Administration, May 4, 2020. Accessed December 20, 2020. https://www.archives.gov/founding-docs/constitution-transcript.

Williams, Lauren C. "National Guard Taking Expanded Election Support Role in 2020." *Federal Computer Week*, November 2, 2020. Accessed December 20, 2020. https://fcw.com/articles/2020/11/02/williams-national-guard-election-cyber.aspx.

Woodward, Calvin. "2 Impeachment Trials, 2 Escape Hatches for Donald Trump." Associated Press, February 14, 2021. Accessed 28 February 2021, https://apnews.com/article/donald-trump-trials-coronavirus-pandemic-mitch-mcconnell-elections-4d1d7ec837c3e942dcbfda962a6dd691.

Xinhua. "China's Arctic Policy." White Paper, People's Republic of China, Beijing, January 2018. Accessed December 20, 2020. Accessed 28 February 2021, http://english.www.gov.cn/archive/white_paper/2018/01/26/content_281476026660336.htm.

Zakrzewski, Cat, and Rachel Lerman. "The Election Was a Chance for Facebook and Twitter to Show They Could Control Misinformation. Now Lawmakers Are Grilling Them on It." *The Washington Post*, November 17, 2020. Accessed 28 February 2021, https://www.washingtonpost.com/technology/2020/11/17/tech-hearing-dorsey-zuckerberg/.

Zeigler, Sara L. "Communications Decency Act of 1996." *The First Amendment Encyclopedia*, 2009. Accessed December 20, 2020. Accessed 28 February 2021,

https://www.mtsu.edu/first-amendment
/article/1070/communications-decency-act-of-1996.

Zuckerberg, Mark. “Four Ideas to Regulate the Internet.” Facebook, March 30, 2019. Accessed 28 February 2021, https://about.fb.com/news/2019/03/four-ideas-regulate-internet/?utm_source=ads.