REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
28-05-2021	Master's Thesis	August 2020-May 2021

4. TITLE AND SUBTITLE
Big Help or Big Brother:
Understanding the Legal Parameters of Domestic Military Operations in the Information Environment

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Hartman, Benjamin, R
Commander, United States Navy

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Joint Forces Staff College- NDU/ Joint Advanced Warfighting School
7800 Hampton Blvd
Norfolk, VA 23511

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution is unlimited.

13. SUPPLEMENTARY NOTES
Information as of 01 MAY 2021.

14. ABSTRACT

The development of digital medias has led to a resurgence of Operations in the Information Environment. Many of the recent incidents of civil unrest were incited and fueled by the distribution of information across medias from both foreign and domestic actors. Essentially, the US faces three interrelated challenges. The US faces malign actors who have weaponized the information environment, the United States Government (USG) lacks a coherent strategy to contest the information environment, in part because the legal roles and authorities for the various organizations for operating in the information environment, and it is not clear, according to domestic and international law, what retribution states can respond with to acts in the information environment. An examination of Operations in the Information Environment to contest and combat disinformation and propaganda from foreign actors designed to influence the US population and exacerbate the ramifications of existing social issues requires an understanding of the legal limitations, and of the tactics of disinformation campaigns. The USG should engage the US citizens in a digital literacy program designed to increase the cognitive ability of its population to recognize disinformation. US Northern Command should lead a joint task force responsible for the dissemination of Strategic Communications contesting disinformation and propaganda, as well as provide the framework for cooperation between government agencies and private corporations in the recognition of disinformation and propaganda campaigns and to assist law enforcement in contesting the campaigns targeting domestic audiences.

15. SUBJECT TERMS
Operations in the Information Environment, Information Warfare, International Law

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**b.THIS PAGE**	Unclassified Unlimited	**48**	**19b. TELEPHONE NUMBER** *(Include area code)* 757-443-6252
U	**U**	**U**			

NATIONAL DEFENSE UNIVERSITY

JOINT FORCES STAFF COLLEGE

JOINT ADVANCED WARFIGHTING SCHOOL

Big Help or Big Brother: Understanding the Legal Parameters of Domestic Military Operations in the Information Environment

by

Benjamin Hartman

CDR, USN

This work cannot be used for commercial purposes without the express written consent of the author.

Page Intentionally Left Blank

Big Help or Big Brother: Understanding the Legal Parameters of Domestic Mi
Operations in the Information Environment

by Benjamin Hartman
CDR, US Navy

A paper submitted to the Faculty of the Joint Advanced Warfighting School
partial satisfaction of the requirements of a Master of Science Degree in Joi
Campaign Planning and Strategy. The contents of this paper reflect my ow
personal views and are not necessarily endorsed by the Joint Forces Staff Colle
the Department of Defense.

This paper is entirely my own work except as documented in footnotes.

Signature: _____

Date: 28 MAY 2021

Thesis Advisor:

Signature: _____
Jeffrey Turner, MFA
Instructor

Approved by:

Signature: _____
Miguel L. Peko, Captain, US Navy
Director, Joint Advanced Warfighting S

Page Intentionally Left Blank

Abstract

The development of digital medias has led to a resurgence of Operations in the Information Environment. Many of the recent incidents of civil unrest were incited and fueled by the distribution of information across medias from both foreign and domestic actors. Essentially, the US faces three interrelated challenges. The US faces malign actors who have weaponized the information environment, the United States Government (USG) lacks a coherent strategy to contest the information environment, in part because the legal roles and authorities for the various organizations for operating in the information environment, and it is not clear, according to domestic and international law, what retribution states can respond with to acts in the information environment. An examination of Operations in the Information Environment to contest and combat disinformation and propaganda from foreign actors designed to influence the US population and exacerbate the ramifications of existing social issues requires an understanding of the legal limitations, and of the tactics of disinformation campaigns. The USG should engage the US citizens in a digital literacy program designed to increase the cognitive ability of its population to recognize disinformation. US Northern Command should lead a joint task force responsible for the dissemination of Strategic Communications contesting disinformation and propaganda, as well as provide the framework for cooperation between government agencies and private corporations in the recognition of disinformation and propaganda campaigns and to assist law enforcement in contesting the campaigns targeting domestic audiences.

Page Intentionally Left Blank

Table of Contents

Chapter 1: Introduction

The development of digital medias has led to a resurgence of Operations in the Information Environment (OIE). Many of the recent incidents of civil unrest in the US were incited and fueled by the distribution of information across medias from both internal and external actors. The United States disposition towards freedom of speech and freedom of the press make it difficult for authorities to ensure those freedoms are not infringed while contesting disinformation and the negative influence in the information environment. Yet, despite the need for action, it is unclear whether military forces can legally employ Operations in the Information Environment within the borders of the United States.

In one regard, the limitations on military power stem from the Constitution. The founders of the United States were wary of any one branch of government becoming too powerful. An executive branch that would be controlled by one individual could become an authoritarian ruler with the control of the Armed Forces. History is littered with military coups that have undermined the will of the people and given an individual in control of the military supreme command. The founders of the United States did not want to trade the monarchy of the United Kingdom for an American monarchy. The Constitution is written in a way that established checks and balances on the different branches in order to maintain a government for the people and by the people. The same checks and balances prescribed in the Constitution that provide protection from a dictator, also establish the legal framework that limits what the Armed Forces can do domestically.

United States Northern Command (USNORTHCOM) is the Department of Defense's primary command responsible for the Area of Responsibility that contains the United States. NORTHCOM's primary mission is to provide command and control of DOD homeland defense efforts and to coordinate Defense Support to Civil Authorities (DSCA). When an emergency or crisis exceeds local, state, and federal agencies, USNORTHCOM can be tasked with supporting the government agencies that require assistance. USNORTHCOM may be tasked with DSCA during natural disasters, counter-drug operations, or terrorist attacks.

The United States military has fought many of its battles overseas, but Operations in the Information Environment (OIE) occur both on foreign soil and domestically. Yet, the use of digital medias to target the citizens of a country in the information environment pose a legal obstacle since the law is unclear about jurisdiction and whether Operations in the Information Environment constitute acts of war. Information transmitted across borders can be used to accomplish military objectives. The spreading of disinformation can be done by state or non-state actors, which determines how the country receiving the information can respond. In most cases, the norms for cyber activities and disinformation campaigns are unclear in the definition of what constitutes war or allows an act of force in response.[1] The difficulty of attribution in cyber events further complicates the problem.[2] The adversaries of the United States are attempting to take advantage of the gaps and seams that civil unrest, riots, and insurrections provide. Malign actors are using

[1] Michael J. Adams and Megan Reiss, "International Law and Cyberspace: Evolving Views," *Lawfare*, March 4, 2018, https://www.lawfareblog.com/international-law-and-cyberspace-evolving-views.

[2] Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections,* January 6, 2017.

the information environment by disseminating propaganda and disinformation to create and sow chaos within the United States.

Essentially, the US faces three interrelated challenges. First, it faces actors who have weaponized the information environment. Second, the USG lacks a coherent strategy, in part because the legal roles and authorities for the various organizations, particularly the DOD, for operating in the information environment and synchronizing the various instruments of power to counteract the propaganda being created in order to sow chaos within the United States.[3] Third, while the US certainly has the resources and capabilities to contest the information environment, it is not clear, according to domestic and international law, whether acts in the information environment constitute sufficient cause for declarations of war or an act of force in order to deter future operations. In order to counter the foreign actors, the USG must first understand the tactics malign actors use to foment potential uprising and why disinformation campaigns are able to be effective in influencing groups of people.

A Whole of Government approach is required to counteract the use of disinformation and propaganda to lessen the influence it has on the citizens of the United States in creating and increasing the frequency and severity of civil unrest. Digital medias provide malign actors with the tools required to bury the truth in disinformation. The rush to report a story has led to news reporting that does not meet the verification requirements of professional journalists. The two factors combine to make disinformation more effective in influencing the citizens of the United States. It is

[3] Congressional Research Service, *Information Warfare: Issues for Congress,"* March 5, 2018, https://crsreports.congress.gov/product/pdf/R/R45142/5.

unlikely that restrictions on media and speech would be instituted, so the responsibility is on the consumer of the information to determine its legitimacy. The US should follow the lead of its European allies in promoting digital literacy for its citizens to increase the cognitive abilities to discern propaganda and questionable sources. USNORTHCOM should lead the dissemination of strategic communications during times of civil unrest and be the coordinating authority for increased cooperation between the private sector and government agencies. This cooperation can be utilized in times of crisis to help restore order while not infringing on the rights and freedoms of US citizens.

The Constitution of the United States, supported by United States Code Title 10, gives USNORTHCOM the legal authority to assist law enforcement in the subduing of riots and lessening the severity of civil unrest. The USG has an obligation and legal authority to combat false narratives and disinformation by conducting Operations in the Information Environment from both foreign and domestic sources.[4] The USG has the authority to use law enforcement and the military, when law enforcement lacks the resources or personnel, to counteract the use of disinformation and false narratives that foment violence and civil unrest. USNORTHCOM is legally permitted to assist in the synchronizing of various instruments of power to counteract the disinformation and misinformation propagated in the information environment by foreign entities. Cyber actors have utilized domestic sources to disseminate disinformation which complicates the attribution and authorities given to military personnel to combat the disinformation. USNORTHCOM can provide law enforcement with the capabilities and personnel to provide the Information Related Capabilities in the dissemination of strategic

[4] U.S. Code 10, Section 397.

communications. The Armed Forces can provide the near real time assessments and media products to establish the narrative.

Social media platforms can flag or remove posts that disseminate false or misleading information. Social media companies have threat intelligence teams that monitor for misuse of the platform and criminal behavior.[5] The threat intelligence teams from Facebook reported a disinformation campaign in 2015 by the Islamic Revolutionary Guard Corps of Iran against the US Department of State.[6] The framework exists for cooperation between social media platforms and law enforcement, the requirements should be codified in order to maintain transparency and freedom from misuse. Yet, Facebook has banned law enforcement from using software for large scale collection and analysis of user data.[7] Times of crisis, when law enforcement is overwhelmed with riots or violent civil unrest, create the requirement for the Armed Forces to conduct Operations in the Information Environment to assist law enforcement in lessening the severity of the crisis. The government agencies lack the oversight of the social media platforms used to disseminate the disinformation. The coordination between the social media gatekeepers and law enforcement needs to be further developed and a framework established to be used during times of crisis. The framework exists for reporting of illegal activities and times of crisis necessitate the use of all available tools to target efforts to foment violence.

[5] Lawfare Podcast. "Alex Stamos on the Hard Tradeoffs of the Internet." Produced by Jen Patja Howell. February 13,2020. 04:41, https://www.lawfareblog.com/lawfare-podcast-alex-stamos-hard-tradeoffs-internet.

[6] Lawfare Podcast, 05:00.

[7] Jeff Horwitz and Dustin Volz, FBI Surveillance Proposal Sets Up Facebook Clash, Wall Street Journal, August 9, 2019.

Methods

The research conducts a legal review of the Armed Forces assisting law enforcement within the United States to prevent and lessen civil unrest initiated by foreign and domestic entities. The research divides legal findings into three categories: prohibited activities, permitted activities, and activities that are in the grey area. The legal research also considers international law with digital medias that operate irrespective of political boundaries. An in-depth study of propaganda and disinformation campaigns provides a framework for understanding what objectives the actors are trying to achieve with activities in the information environment. Once the objectives are understood, the USG can create a strategy to counter malign actors in the information environment. In a case study, examination of how the information environment was used by foreign actors in the 2016 US Presidential Campaign.

The legal analysis for conducting Operations in the Information Environment is tied to the use of the military in assisting law enforcement. Title 10 of the United States Federal Code establishes the baseline for what is prohibited and permitted for use of the armed forces. The research for the prohibited activities focuses on the Posse Comitatus Act, Smith-Mundt Act, and the Law of Armed Conflict. The activities that are permitted are grounded in research on the Insurrection Act, the National Defense Authorization Act of 2019, and the US Cyber Strategy. The activities that potentially could be conducted exist outside what is expressly prohibited by domestic and international law.

The Insurrection Act and the Posse Comitatus Act are the basis for using the military to assist law enforcement domestically and ensuring the military is not overused to intimidate or restrict life inside the United States. The Insurrection Act is incorporated

in Section 331-335 of Title 10 U.S.C. The Posse Comitatus Act limits the President's authority to use the military to act in a law enforcement role. The Act was drafted to end the use of federal troops from policing state elections in the former Confederate states. The troops were deployed to prevent intimidation and unlawful restriction at polling sites.

The legal analysis must also consider international law due to the ability of digital media actors to cross international boundaries quickly and easily. The United States Department of Defense *Law of War Manual* requires a distinction between combatants and civilians. Combatants must be trained in the law of war, serve under effective discipline, and be under the command of officers responsible for their conduct.[8] The 1907 Hague Convention Respecting the Rights and Duties of Neutral powers and Person in case of war limits the ability of governments to respond to non-state actors or cyber criminals routing their signal through unsuspecting host countries.

The 2016 Presidential Election provides an example of influence operations across modern forms of digital medias. The advent of social media has created new liabilities in the information environment. The disinformation campaigns and dissemination of information to targeted individuals to influence or persuade the election results display how the cyber domain and information environment can be leveraged by malign actors. The difficulty of attribution of cybercrimes and the challenges with international laws and norms present challenges that the USG must confront in the grey zone. The legal findings help determine the capabilities that can be used to counteract

[8] US Department of Defense, Office of the General Counsel, *An Assessment of International Legal Issues in Information Operations,* by Philip A. Johnson, May 1999. https://fas.org/irp/eprint/io-legal.pdf.

disinformation campaigns. The case study provides a real-world example of tactics of disinformation campaigns and vulnerabilities.

Chapter 2: Legal Research

The role of the Armed Forces of the United States in domestic operations involving law enforcement has been an issue for the USG since the establishment of the Constitution. The colonies experienced injustices and abuse of power by the British Army that left them leery of standing militaries. The experience encouraged the founders to create the *Bill of Rights* as part of the founding of the nation. The threat of a military coup or abuse of power by the executive branch has been a part of history for many nations and the founders wanted to ensure steps were taken to protect the citizens and the democratic processes through the rule of law. Over the course of the nation's history, from its onset to the current day, several protections have been implemented to limit the use of military forces.

The advent of digital medias has exposed further legal issues because they operate irrespective to political boundaries. International law poses another obstacle for both the military and law enforcement to combat the use of the cyber domain by actors attempting to foment violence and unrest inside the United States from both inside its borders and internationally. The International Court of Justice and the Law of Armed Conflict attempt to define international norms on how it is appropriate for a state to respond to cyberattacks. The norms are not clear on cyber or information attacks and what the kinetic equivalent of the attacks could or should be.[1]

[1] Duncan B. Hollis, "Why States Need An International Law for Information Operations," *Lewis and Clark Law Review,* Lewis and Clark Law School, December 5, 2007, pg 1026, https://law.lclark.edu/live/files/9551-lcb114art7hollis.pdf.

The complexity of the nexus between international and state law, as well as domestic and foreign security issues, creates an environment that requires understanding the established rules and norms for what constitutes the equivalent to a kinetic attack in the cyber domain or the information environment and an organizational construct that allows freedom of movement for those military or law enforcement entities to work in unison across domains and with the appropriate tools. The following two sections highlight the domestic and international laws that have set clear boundaries for what is allowed and not allowed by domestic U.S. laws. The third section highlights the grey space between what is expressly prohibited and what is explicitly allowed.

Prohibited Activities

Title 10 of the United States Federal Code establishes the standard for how and when the Armed Forces of the United States can be used. Title 10 restricts the direct participation of a member of the armed services to actively support civilian law enforcement agencies.[2] Civilian law enforcement personnel are trained in search, seize, or arrest activities in compliance with the US Bill of Rights, Fourth Amendment. The protections against illegal searches and seizures afforded by the Fourth Amendment require the appropriate training and jurisdictional authority for all enforcement of laws to be legally binding. The legislative branch of the USG has imposed additional restrictions on the use of the military in law enforcement through the Posse Comitatus Act.

The United States experienced a tumultuous time during the 1860's. The divided country had to find a way to reestablish the Union after the bloody Civil War. As part of

[2] US Code 10, Section 275.

ensuring the democratic process continued, the Armed Forces deployed to polling sites during the Civil War reconstruction to ensure full participation of those with voting rights.[3] The advantage of federal troops over local law enforcement was not only the loyalty of the military to the Constitution but an enforcement mechanism for those that did not follow the orders that local law enforcement did not have. The use of soldiers to enforce voting rights was the first of two events that led to the passage of the Posse Comitatus Act of 1878.

The second impetus for the Act originated from the law enforcement fort commanders imposed on western territories.[4] The fort commanders were violating settlers' constitutional rights with the imposition of law enforcement consequences without due process. The two events garnered enough support in Congress to pass the Posse Comitatus Act that prohibited the Army from executing the law unless allowed by the Constitution or Congress. Case law indicates that the act is violated when military investigators are used, the military "pervades the activities" of civilian officials, or the military is used so as to subject the "citizens to the exercise of military power which was regulatory, prescriptive, or compulsory in nature."[5] Posse Comitatus seeks to limit the infringement of state authorities by federal authorities using military personnel.

The Smith-Mundt Act of 1948 was enacted to enable the Department of State to disseminate informational products in Europe that would counter the Soviet propaganda.[6]

---

[3] Bonnie Baker, *Origins of Posse Comitatus,* https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/baker1.pdf.

[4] Baker, *Origins of Posse Comitatus.*

[5] Elsea, The Posse Comitatus Act and Related Matters: The Use of the Military to Execute Civilian Law.

[6] Matt Armstrong, "A Brief History of the Smith-Mundt Act and Why changing it matters"; MountainRunner. Us (blog). Feb 23,2012. https://mountainrunner.us/2012/02/history_of_smith-mundt/.

The Cold War had brought information activities into the public view. The dissemination of information intended for foreign audiences to win the information war against the Soviet Union was deemed not appropriate for domestic consumption. Congress was wary of any attempt to influence the citizens of the United States via propaganda and appearing to operate on the same level as the Communist government.

The Smith-Mundt Act is incorporated into Title 22 of the U.S.C. and limits what the Department of State (DoS) can do geographically with DoS information campaigns.[7] The Act was aimed at the United States Information Agency and other federal entities that ran programs like Voice of America and radio programs broadcast to Cuba. The Smith-Mundt Act was amended in 2012 but the Department of State is the only entity listed in the legislation. The original intent was for the information that was being disseminated to be tied into public diplomacy.[8] Therefore, with the closure of the United States Information Agency, DoS would be the primary responsible agent.

The OIE conducted utilizing the cyber domain require study in international law. Cyber has no respect for international boundaries and the difficulty with attribution creates legal dilemmas.[9] The United Nations charter only prohibits "states," meaning nation-states, use of force.[10] If the crime or act cannot be attributed to a state actor, then a response in self-defense may not be legal in accordance with the UN Charter. The Law of Armed Combat (LOAC) distinguishes between combatants and non-combatants. [11] A state cannot respond with military violence against an individual deemed a non-

[7] Armstrong, "A Brief History of the Smith-Mundt Act and Why changing it matters."
[8] Armstrong, "A Brief History of the Smith-Mundt Act and Why changing it matters."
[9] Hollis, "Why States Need An International Law for Information Operations", pg 1025.
[10] Hollis, "Why States Need An International Law for Information Operations", pg 1040.
[11] Hollis, "Why States Need An International Law for Information Operations", pg 1042-1043.

combatant by LOAC. A person sitting behind a computer in a foreign country may not be deemed a combatant regardless of the level of damage or severity of the act in the cyber domain. The DOD Office of General Counsel believes the consequences of the attack are likely to be more important than the means used when determining if it constitutes an armed attack.[12] The attribution of the attack to a non-combatant would still severely limit what a state can do in response for an attack according to LOAC, no matter how severe.

The dual use nature of the OIE equipment make it more difficult to use the Law of War or Law of Armed Conflict as the legal authority for retribution. By 2000, 95% of military traffic moved over civilian communication and computer systems.[13] The 1907 Hague Convention on Respecting the Rights of Neutral Powers and Persons in Case of War protects neutral powers that may or may not be aware of what their communication systems are being used for.[14] The once clear lines between domestic and foreign security threats are gone. The combination of foreign and domestic security threats requires greater cooperation between federal agencies, such as federal law enforcement and the military. No single agency is capable of being responsible for all the threat areas.[15]

[12] US Department of Defense, Office of the General Counsel, An Assessment of International Legal Issues in Information Operations, by Philip A. Johnson, May 1999, 18.

[13] Hollis, "Why States Need An International Law for Information Operations", pg 1044.

[14] US Department of Defense, Office of the General Counsel, *An Assessment of International Legal Issues in Information Operations.*

[15] Roger Z. George and Harvey Rishikof, "The National Security Enterprise: Navigating the Labyrinth", 2ndEdition, Washington, D.C.: Georgetown University Press, 2017, pp 382-400.

Permitted Activities

The Constitution calls for "establishing justice, ensure domestic tranquility, provide for the common defense and promote the general welfare."[16] The Constitution requires a standing Army and Navy, which establishes the tools to achieve those ends.[17] The Constitution explicitly gives the authority to the USG to utilize the military to suppress insurrections.[18] The Constitutional authority were further codified by the Insurrection Act of 1807. The President can use the military at the request of the state legislature or its governor.[19] The President has used the Presidential authority in reaction to national disasters, civil rights issues, and riots. Governors requested federal assistance in 1992 for the riots in Los Angeles and in 2015 for the aftermath of Hurricane Katrina in New Orleans. The President can also use the military to enforce federal law and to protect civil rights, according to the Insurrection Act.[20] The Act has incurred both state approval and disagreement, as was observed in Portland, Oregon in 2020. Without the governor or state legislature's request, federal law enforcement was deployed to protect federal buildings and monuments.[21]

Title 10 allows for the Secretary of Defense to make available any equipment or facility to law enforcement for official law enforcement purposes.[22] The military can also assist with reconnaissance, detection, and monitoring. The relationship is established

[16] US Constitution, Preamble.
[17] U.S. Constitution, art 1, sec 8.
[18] US Constitution art I, sec 8.
[19] Elsea, *The Posse Comitatus Act and Related Matters: The Use of the Military to Execute Civilian Law*.
[20] 10 USC 251
[21] Mike Baker, Thomas Fuller, and Sergio Olmos, "Federal Agents Push into Portland Streets, Stretching Limits of Their Authority," *New York Times*, July 25, 2020. https://www.nytimes.com/2020/07/25/us/portland-federal-legal-jurisdiction-courts.html.
[22] US Code 10, section 272.

and being utilized for combatting the illegal drug trade. Joint Task Force North is a subordinate unit to USNORTHCOM and provides counter narcotic support to law enforcement with specialized capabilities.[23] The task force assists other federal agencies as well as state and local law enforcement in counterdrug operations.

Congress has affirmed that operations of military personnel in cyberspace are operations short of war.[24] Activities as part of operations short of war include information operations and deterrence of hostilities.[25] The Congressional Declaration concerning cyberspace operations means they are not subject to the War Powers Resolution Act that negates the requirement for Congressional approval.[26] The National Defense Authorization Act of 2019 authorized the executive branch to conduct appropriate and proportional actions in foreign cyberspace to disrupt, defeat, and deter.[27] OIE uses cyberspace to create hostilities and foment violence. If the source cannot be identified or can be denied as part of a state agency, LOAC does not apply, and therefore becomes a law enforcement issue across political boundaries.[28] However, the US Cyber Strategy states it will use all available instruments of power against state and non-state actors.[29] With the authorities granted by Congress and the guidance given in the Cyber

[23] Johnny D. Sellers Jr. and Danielle Adair, "The Department of Defense's Support to Law Enforcement Agencies in Countering Drug Trafficking," *The Police Chief* 82 (August 2015): web-only, http://www.policechiefmagazine.org/the-department-of-defenses-support-to-law-enforcement-agencies-in-countering-drug-trafficking/.

[24] Robert Chesney, "The Domestic Legal Framework for U.S. Military Cyber Operations", *Lawfare* blog, August 5, 2020.

[25] US Code 10, Section 394.

[26] Robert Chesney, "The Domestic Legal Framework for U.S. Military Cyber Operations", *Lawfare* blog, August 5, 2020.

[27] Chesney, "The Domestic Legal Framework for U.S. Military Cyber Operations."

[28] Hollis, "Why States Need An International Law for Information Operations", pg 1042-1043.

[29] US Cyber Strategy

Strategy, authorities are given to the executive branch to combat and contest malign foreign actors in the information environment utilizing the cyber domain.

Title 10 designates a Principal Information Operations Advisor that is appointed by the Secretary of Defense. The advisor maintains the authority to supervise DoD actions in the OIE and functions as the liaison with the private sector regarding influence activities from malign foreign actors.[30] Congress has affirmed the DoD is authorized to conduct military operations in the information environment to defend the United States and interests of the United States, allowing the DoD to conduct OIE to deter and defend against disinformation attacks and campaigns short of war.[31]

Uncertain Activities

The Lotus principle of international law states that sovereign states can do what they wish if international law does not prohibit the actions.[32] The Lotus principle leaves much of OIE and cyber activities in the grey zone since the rules and norms have not been established. When Russia attacked Estonia via cyber means in 2007, the Russian government denied any involvement.[33] The use of disinformation as part a denial strategy combined with the ability of hackers to manipulate computers remotely or through other countries, creates a complex environment for determining what nation-states can do in response.

US Code gives the Department of Defense the authority to combat malign foreign actors in the cyber domain and within the information environment. The Computer Fraud

[30] 10 U.S.C. Section 397.
[31] 10 U.S.C. Section 397.
[32] Hollis, "Why States Need An International Law for Information Operations," pg 1035.
[33] Hollis,"Why States Need An International Law for Information Operations," pg 1025.

and Abuse Act prohibits the destruction of computers even if the computer was used in a crime.[34] The limitation of physical responses does not limit the use of information as a tool. The Smith-Mundt Act (SMA) does not specifically mention the Department of Defense or Department of Homeland Security. The DoD has chosen to adhere to the SMA even though it is not legally bound to do so.[35] The current context of digital medias compared against the historical stigma that labelled all government communication as propaganda necessitates reconsideration. Government agencies have the framework for oversight and accountability in place to ensure the information being disseminated is not incomplete or misleading but a source for accurate information.

Digital medias have created twenty-four-hour news cycles that flood consumers with information. The DoD has the means to use the same digital medias to provide information to the public to establish a narrative. The SMA was not created to limit the USG from providing the United States citizens information but to enable the USG to contest disinformation and propaganda.[36] Malign foreign actors have been using disinformation to create civil unrest in the US. If the acts can be attributed to a state, then retribution of self-defense is allowed.[37] If the act is attributed to an individual or group of individuals, it necessitates law enforcement involvement rather than military involvement. The blurring of lines between domestic and foreign security threats creates a need for the military to work in cooperation with law enforcement. The relationship already exists in battling the influx of illegal drugs. Homeland Security Directive 8

[34] US Code 18, Section 1030.

[35] Matt Armstrong, DHS, Social Media and the SMA, Sept 2,2019, https://mountainrunner.us/2019/09/dhs-smithmundt/.

[36] Armstong, A Brief History of the Smith-Mundt Act and Why Changing it Matters.

[37] Hollis," Why States Need An International Law for Information Operations", pg 1042-1043.

directs federal assistance in prevention activities, such as information gathering, detection, deterrence, and collaboration related to terrorist attacks.[38] In times of crisis, the President has the authority to leverage the relationships to restore domestic tranquility. In such instances, the military can legally provide the equipment and personnel to conduct information campaigns and assist law enforcement while supporting and defending the US Constitution.

[38] Homeland Security Presidential Directive 8, December 17, 2003.

Chapter 3: Disinformation Campaigns

Sun Tzu stated that the political goal of warfare is achieved by creating chaos in an enemy's society.[1] Mao Tse-tung understood the principle and the importance of using propaganda effectively for influencing the local populations at the beginning of an insurgency. The Soviet Union dedicated a significant amount of effort and financing in the creation of propaganda with the purpose of creating tension within the North Atlantic Treaty Organization during the Cold War. Digital medias have enhanced the ability of propaganda to reach the populations of foreign countries and the quantity and speed of information dissemination.

Digital medias create the opportunity for actors to interfere in societies in ways Sun Tzu did not have available. Operations in the Information Environment (OIE) through digital media provide the capability to influence the population directly, without gatekeepers; on a large scale, given the reach and pervasiveness of digital medias; and the potential to incite specific target populations, using big data and psychometrics aimed at specific users and populations. The capability to influence and mobilize people with a smartphone or computer provides malign foreign actors an audience of millions, if not more. The Islamic State used information to recruit personnel and sow terror and disunion through social media.[2] ISIS was able to create chaos in cities which caused mass defections of police and military members, all through digital medias.

Digital medias are used by malign actors to disseminate propaganda or by producing enough disinformation that the truth is buried. The Russian Internet Research

[1] Edward O'Dowd & Arthur Waldron (1991) Sun Tzu for strategists, Comparative Strategy, 10:1, 25-36.

[2] P.W. Singer and Emerson T. Brooking. Like War The Weaponization of Social Media. New York, New York: Houghton Mifflin Harcourt Publishing Company, 2018, pg 8.

Agency (IRA) used thousands of trolls and tens of thousands of bots during the 2016 Presidential Election, sowing doubt and burying the truth.[3] The trolls and bots created thousands of "likes" that exploited the social media framework to increase the audience and create the perception of truth through popularity. The IRA strategy seeks to capitalize on existing social issues by distorting facts, publishing part of the facts, or using emotional appeals to foment unrest.[4] Trolls are using cyber tools to manipulate social media to establish the narrative and target audiences that are predisposed to be influenced by propaganda that targets specific social issues.

The low barrier for entry allows state and non-state actors to exploit people's cognitive biases, exacerbate political tribalization, and foster distrust with leaders and institutions.[5] Malign foreign actors have the goal of dividing the US population with a firehose of falsehoods and misinformation that takes advantage of pre-existing social divisions.[6] The ability of actors to weaponize information and control the narrative through digital medias brings the battlefield of information warfare to the soldier and the citizen.

Non-state Actors

Non-state actors have been able to compete with traditional state actors through the cyber domain using the information environment. OIE are an effective tool to influence groups of people and organize for a common purpose. Non-state actors have

[3] Singer, Like Wars, pg 16.
[4] Understanding Media and culture, pg 28.
[5] Mad Scientist Laboratory, "Insights from the Mad Scientist Weaponized Information Series Virtual Event," October 19,2020, https://madsciblog.tradoc.army.mil/277-insights-from-the-mad-scientist-weaponized-information-series-of-virtual-events/
[6] Mad Scientist Laboratory, 277.

been able to influence large groups with relative anonymity and with little upfront costs. Mao Tse-tung was a non-state actor with the objective of becoming a state actor using an insurrection of the Chinese government.

Mao Tse-tung wrote his manual for guerrilla warfare in rural China. Mao is regarded as not only leading the revolution against the government of China but creating a framework for future guerrillas to conduct operations. Mao's framework is laid out in three phases, and he suggests successful guerilla leaders spend more time in organization, instruction, agitation, and propaganda.[7] The first phase that Mao recommends is to organize, consolidate, and preserve the revolution. The goal of the first phase is to train and indoctrinate volunteers.[8] The properly trained volunteers are then sent forth as agitators and propagandists to persuade and convince the local populations. The second phase consists of sabotage and terrorism, and the third phase is the destruction of the enemy. First phase activities are the most relevant for OIE because they focus on recruitment and maintaining the favor of the population. Mao recognized that guerilla warfare derives its power from the masses.[9] A revolution requires the support of the local populations to preserve itself. Without the popular support, the guerillas or revolutionaries will be exposed to the existing authorities.

Mao understood the principles put forth by Sun Tzu, believing the mind of the enemy and will of his leaders is the target of far more importance than the bodies of his troops.[10] ISIS used propaganda over social media to recruit and attack the minds of its

[7] Fleet Marine Force Reference Publication (FMFRP)12-18, "MaoTse-tung on Guerilla Warfare", April 5, 1989, pg 8.

[8] Fleet Marine Force Reference Publication (FMFRP)12-18, "MaoTse-tung on Guerrilla Warfare", pg 21.

[9] FMFRP 12-18, pg 44

[10] FMFRP 12-18, pg 23

enemies. The use of threats and terror over social media disintegrated the personnel assigned to the defense of Mosul in northern Iraq.[11] ISIS was able to overtake the city with little difficulty using tweets instead of physical violence. Russia also used the tactic to target the Ukrainian Army tasked with fighting the rebels in Eastern Ukraine.[12] The effects of Mao's principles are amplified by the ability to reach large groups of people by digital medias and to tailor the information to influence the local populations to prepare the battle space in favor of the insurgency. Mao knew the value of propaganda and using personnel in their native localities.[13] Mao labeled them "self-defense groups," and their main purpose was to inculcate the people with military and political knowledge in favor of the revolution.[14] The self-defense groups used in their native locality would know the people and have the credibility to influence the population.

Mao prescribed each large unit to have a printing press and paper to create propaganda.[15] Mao put in place a system that could control the information environment and unite the masses under his ideology. The message was carried by people that had credibility with the local populations, and the message was controlled by the revolutionary leadership. The capability of digital media to not only reach a larger number of people but to target the information to those who are either more apt to be sympathetic to the cause or are geographically being targeted has increased the effectiveness and efficiency of following Mao's guidelines for propaganda.

[11] Singer, *Like Wars*, pg 5-6.
[12] Singer, *Like Wars,* pg 9.
[13] FMFRP12-18, pg 85.
[14] FMFRP 12-18, pg 85.
[15] FMFRP 12-18, pg 85.

Extremists can reach recruits through forums and chatrooms. ISIS can reach U.S. citizens and convince them to be friendly to their cause.[16] The use of OIE to broadcast the grievances that unite people ideologically can be targeted to forums predisposed to accept the information and becomes a powerful recruiting tool. Digital media has exponentially increased the size of the audience extremists and malign actors can reach. The lack of identity enforcement allows for trolls to assume identities that convey credibility to the audience they seek to influence, which incorporates Mao's teachings on how to gain credibility with the local populations to gain the trust of the people. Non-state actors can utilize digital medias to create chaos within the United States while operating below a level that would invoke the LOAC. The low entry cost expands the quantity of malign actors attempting to sow disinformation and technology is increasing the quality of disinformation which in turn increases its influence.

State Sponsored Actors

ussia inherited its familiarity with propaganda and disinformation efforts from the Soviet strategy used during the Cold War. Soviet leaders used the term "active measures" to describe an array of overt and covert techniques for trying to influence people and events.[17] The Soviets used overt propaganda channels and covert oral and written propaganda techniques including international front organizations.[18] Different Soviet government agencies, under the guise of a foreign identity, wrote articles in

[16] Singer, *Like Wars,* pg 170.
[17] Shultz, Richard H., and Roy Godson. 1984. *Dezinformatsia : Active Measures in Soviet Strategy*. Pergamon-Brassey's, pg 2.
[18] Shultz, Richard H., and Roy Godson. 1984. *Dezinformatsia : Active Measures in Soviet Strategy*. Pergamon-Brassey's, pg 2.

foreign publications that would be attributed to non-Soviet authors. Interviews with former KGB and Czechoslovakian Intelligence officers document the ability of the Soviets to recruit and use journalists in other countries to create publications that are favorable to the Soviet Union.[19] One such journalist was Piere Charles Pathe in France.[20] In the 1960's, Pathe wrote many articles and published a newsletter with covert propaganda and disinformation that was sent to a targeted audience.[21] Active measures were conducted in OIE utilizing any available media that could be used to influence populations.

Disinformation, called *dezinformatzia* in Russian, can be defined as false, incomplete, or misleading information passed to a targeted individual, country, or group.[22] The information may contain both true and false information intended to deceive the recipient. In July of 2014, a commercial flight from the Netherlands to Malaysia crashed in Eastern Ukraine. The Malaysian flight was shot down by a Russian surface-to-air missile system being operated by Russians in support of the Ukrainian rebels.[23] Both the Ukrainian government and the Russian backed separatists blamed each other for the tragic accident to avoid taking responsibility that would endanger public support for their cause.[24] The truth was hidden in a swirling fog of theories across social media.[25] The theories the Russian government proposed each had a hint of truth to them, making it very difficult to determine what happened and who was responsible.

---

[19] Shultz, Richard H., and Roy Godson. 1984. *Dezinformatsia, pg 168.*
[20] Shultz, Richard H., and Roy Godson. 1984. *Dezinformatsia, pg 136.*
[21] Shultz, Richard H., and Roy Godson. 1984. *Dezinformatsia, pg 136.*
[22] Shultz, Richard H., and Roy Godson. 1984. *Dezinformatsia : Active Measures in Soviet Strategy*. Pergamon-Brassey's, pg 38.
[23] Singer, *Like Wars*, pg 74-75.
[24] Singer, *Like Wars*, pg 72.
[25] Singer, *Like Wars*, pg 72.

Russia also used the difficulty of attribution, the inability to definitively attribute an attack, in the cyber domain to further confuse investigators. Russia was able to geographically target the Ukrainian Army units arriving at the front lines with disinformation and threats via their smartphones.[26] Russia, much like ISIS, was able to attack the minds and morale of their adversaries with a Sun Tzu-like strategy.

The Soviets also used international front organizations to further their propaganda. The Vietnam Support Committee in the United States was Soviet run and funded.[27] The committee would encourage people not to honor the draft during the Vietnam War and used pictures of those avoiding the draft for international propaganda.[28] Social media has created new avenues for the Russians to use this technique, such as in the 2016 U.S. Election.

The international front organizations were not the only forgeries. The Soviet Union also created forgeries that took the form of authentic looking but false US government documents.[29] The forged documents were used to bring discord between the Western European nations and the US. Digital medias have created new opportunities for forgery whether it is a commercial airliner with an altered image of a Ukrainian military jet behind it or editing videos to show partial truths that sow discontent. Russia has used RT, formerly Russia Today, and Sputnik to broadcast stories promoting dissatisfaction with the USG through websites and social media.[30] The overt news stories appear authentic and of American origin, but the author's biography lists RT and Sputnik as

[26] Singer, *Like Wars*, pg 59.
[27] Shultz, Richard H., and Roy Godson. 1984. *Dezinformatsia, pg 120.*
[28] Shultz, Richard H., and Roy Godson. 1984. *Dezinformatsia, pg 125.*
[29] Shultz, Richard H., and Roy Godson. 1984. *Dezinformatsia,* pg 153.
[30] DNI, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution.*"

employers.[31] Just as with Malaysian Flight 17, the news stories do not have to be complete forgeries, the story can contain enough truth to be plausible and the true sources buried where few people will look to verify the authenticity.

Operations in the Information Environment are not new tactics, OIE is being conducted with modern means to increase its effectiveness. Sun Tzu promoted causing chaos in the adversary's society, and Russia has been using OIE since the beginning of the Cold War. The tools that digital media, especially social media, provides malign foreign actors to cross political boundaries to sow discord creates a battlefield beyond the traditional combatants.

[31] From a news story I received through social media regarding election software promoting distrust with the process.

Chapter 4: The 2016 Presidential Election Case Study

The 2016 Presidential Election uncovered some vulnerabilities in the way the United States Government approaches the information environment. The information environment during the election also revealed new vulnerabilities that digital medias create regarding how information can be disseminated, and the influence disinformation can have. The OIE during the 2016 Election cycle provides a historical example of how social media can be used to weaponize information and the lack of will, strategy, and capability for the USG to compete in the information environment.

The evolution of media from word of mouth to the digital age has exponentially increased the amount of people that can receive information and at what speed. Digital medias provide the capability to broadcast information immediately after an event happens or even during the event. The ability of anyone with a cell phone and a social media account to broadcast their version of an event as it is happening is reducing or eliminating the probability that a story is coherently checked for legitimacy. The competition between journalists to break a story or a social media post to set the narrative creates an environment in which being the first to post the story has become more important than confirming and verifying the veracity of the story.

The number of sources available through digital medias and the twenty-four-hour news cycle makes it hard to separate news from entertainment.[1] The blurring of lines between news reporting and entertainment combined with news not having the time to be checked for accuracy creates distrust regarding what sources to believe. Digital news

[1] Author Removed. "Understanding Media and Culture: An Introduction to Mass Communication." University of Minnesota, 2016.

sources and social media make it difficult to keep a secret or hide an event, but it also makes it hard to discern truth from fiction.[2] Russia took advantage of the downing of a commercial airliner over Ukraine, and it used the endemic, systemic obscuration of the facts to sow doubt in the US election.[3] Russia used thousands of trolls and tens of thousands of bots, through state sponsored organizations like the Internet Research Agency, to flood social media with information and disinformation.[4] Each human troll allied themselves with multiple social media accounts that assumed American identities. The bots, automated social media accounts that mimic humans, were able to multiply the dissemination of information and create thousands of" likes" to make the information appear that much more legitimate.[5] Propaganda often distorts the facts, selectively presents facts, or uses emotional appeals to influence or persuade.[6]

Propaganda disseminated through digital media can be targeted to groups through tools created by Facebook and through "cyberbalkanization."[7] Cyberbalkanization is the selection of custom news feeds that only receive the type of information the user wants.[8] Facebook's Core Audience Tool allowed the trolls to identify who would be the most responsive to certain advertisements and ensured the information reached that audience.[9] 126 million Americans were exposed to Russian trafficked content on Facebook during the 2016 Presidential election campaign while 138 million Americans voted in the 2016

[2] Singer, *LikeWars*, pg 82.
[3] Singer, *Like Wars, pg 16.*
[4] Singer, *Like Wars,* pg 16.
[5] Singer, *Like Wars,* pg 16.
[6] Author Removed, "Understanding Media and Culture: An Introduction to Mass Communication."
[7] Author Removed, "Understanding Media and Culture: An Introduction to Mass Communication."
[8] Author Removed, "Understanding Media and Culture: An Introduction to Mass Communication."
[9] Author Removed, "Understanding Media and Culture: An Introduction to Mass Communication."

Presidential election.[10] The cyberbalkanization type of targeting of audiences gave additional tools for overt disinformation sources, like RT and Sputnik, to increase effectiveness.

Cyberspace makes attribution difficult but not impossible.[11] The issue of attribution for the 2016 Election interference is part of the legal problem with the USG's response. The use of trolls and bots was traced back to the Internet Research Agency (IRA), which operates out of Saint Petersburg, Russia.[12] The IRA does not operate as an agency of the Russian government but is financed by a Putin ally.[13] The relationship creates the grey space between state and non-state actor. Russian leadership can use just enough plausible deniability for Russia not to be blamed. As a result of the social media manipulation in 2015, Facebook increased the enforcement of identity requirements.[14] The policy change made it harder for trolls to spread the propaganda through social media profiles, but malign foreign actors can still target groups with propaganda through overt sources. In the 2018 Congressional election, Russia used hundreds of trolls to post false news stories and socially divisive content over social media.[15] Social media users can post things that may not be able to be broadcast by traditional media. The government has lost the ability to censor or regulate nontraditional media sources. The

[10] Post Election 2016 Recap & Resources, last updated August 28, 2020, https://guides.libraries.psu.edu/post-election-2016/voter-turnout.

[11] DNI, Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution."

[12] DNI, Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution."

[13] DNI, Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution."

[14] Lawfare Podcast. "Alex Stamos on the Hard Tradeoffs of the Internet." Produced by Jen Patja Howell. February 13,2020. 32:51, https://www.lawfareblog.com/lawfare-podcast-alex-stamos-hard-tradeoffs-internet.

[15] Congressional Research Service, Election Security: Issues in the 2018 Midterm Elections, by Catherine Theohary and Eric Fischer, August 16, 2018.

movement away from centralized mass media that included regulation to a preference for speed of breaking news accompanied with the decentralized social media structure allowed social media companies to act as a pseudo-government in the role of censorship.[16] While Facebook has teams of analysts that search through content and censor or label posts that may be inaccurate, which helps contest disinformation, they were also caught off guard if not reluctant to serve in the gatekeeper role because it suggested they were censoring user content and speech.[17] The authority gained by social media companies amplifies the shortcomings of the USG position in which it is unwilling or unable to confront issues in the information environment.

The United States Cyber Strategy states, "the US will use all available instruments of power to expose and counter the flood of online malign influence and information campaigns and non-state propaganda and disinformation."[18] The Cyber strategy was signed after the 2016 Election and gives authority to United States Cyber Command to expose and counter either Russia or the IRA. There are no domestic laws that would hinder US Cyber Command from responding in kind to disinformation campaigns or malign cyber activities.[19] The 2019 National Defense Authorization Act authorizes the executive branch to conduct appropriate and proportional action in foreign cyberspace in order to disrupt, defeat, and deter malign foreign actors operating in the information environment.[20] Despite the authority, Russian disinformation campaigns have yet to be deterred. The authorization through the 2019 NDAA gives authority to

[16] Lawfare Podcast. "Alex Stamos on the Hard Tradeoffs of the Internet," 04:41.
[17] Lawfare Podcast. "Alex Stamos on the Hard Tradeoffs of the Internet," 31:49.
[18] US Department of Homeland Security, *Cybersecurity Strategy,* May 15, 2018.
[19] Chesney, Domestic legal framework for U.S. Military Cyber Operations.
[20] Chesney, Domestic legal framework for U.S. Military Cyber Operations.

the military to contest malign foreign actors in this environment but highlights the lack of effectiveness in the deterrence of activities in the information environment.

The USG is authorizing federal agencies to contest the cyber domain, but it has not contested OIE. The USG has regulations on television and other traditional forms of media, but social media platforms have assumed regulatory provisions over the information environment. China has taken over its social media with WeChat, and Chinese citizens are required to have the application while all content is monitored by the government.[21] Such intrusive efforts are not an option for the USG, which raises the concern that the USG has neither the willingness to contest disinformation nor the desire to put in place the requirements to lessen the influence of information campaigns.

[21] Singer, *Like Wars*, pg 51.

Chapter 5: Conclusion

The adversaries of the United States are using the information environment to foment unrest and capitalize on social issues inside the US. The use of disinformation and propaganda through digital medias and social media requires the USG to respond in order to detect and deter malign foreign actor's efforts. Digital media has created vulnerabilities in the information environment and has lessened the influence the USG has over traditional media. Social media corporations have assumed influence over content and become reluctant gatekeepers. The change in relationship will require new strategies and a level of cooperation between the government and private sector in order to successfully contest the information environment from both state and non-state actors.

The USG's strategy should utilize a three-pronged approach of Strategic Communication, a digital literacy education program, and cooperation between law enforcement and the private sector to contest the information environment. USNORTHCOM can fulfill its role in Defense Support to Civil Authorities (DSCA) in providing personnel and capabilities to law enforcement while executing its primary mission of Homeland Defense by deterring or defeating malign foreign actors in the information environment. The threat that state and non-state actors, such as Russia and the IRA from Russia, pose to the United States constitute the weaponization of information that requires a response whether it is a domestic or foreign threat.

Strategic communications alone will not have a drastic impact. The ability to generate a firehose of disinformation may drown out the truth.[1] The ability to construct

[1] Mad Scientist Laboratory.

a narrative with social media in the face of comprehensive reports and investigations has proven difficult to unseat. USNORTHCOM can fill the role of an impartial and credible source of events when the military is involved or as a part of a military and law enforcement partnership. The Department of Defense should utilize its credibility with the American people to disseminate strategic communications in times of civil unrest. During the Vietnam War, General Westmoreland briefed reporters from the US Embassy after it was attacked during the Tet offensive. His assessment did not match the blood-stained lawn in the background of the interview.[2] The media did not understand why Westmoreland claimed the defeat of the Tet offensive was such a success, the media carried a different narrative in its reporting and the General lost credibility with the press corps and the American public.[3] A uniformed USNORTHCOM spokesperson can present strategic communications, but the narrative must be supported by truth in order to maintain the trust and confidence of the public.

The second line of effort should be a digital literacy program for US citizens. Peter Singer in *Like Wars* recommends inoculating society against information threats.[4] The countries that face a constant barrage of information threats from Russia, like Estonia and Lithuania, conduct citizen education programs, public tracking and notices of disinformation campaigns, and legal action against super-disinformation-spreaders.[5] Such a comprehensive digital literacy and strategic communication effort will require a whole of government approach to teach the American public to speak the new language of the digital age. The digital literacy program should incorporate open-source research

[2] Peter Braestrup, *Big* Story, (Novato, CA: Presidio Press, 1994) 122.
[3] Braestrup, *Big* Story, 122.
[4] Singer, *Like Wars,* 263.
[5] Singer, *Like Wars*, 263.

techniques and critical thinking towards the evaluation of sources and biases.[6] While terms like "fake news" have been overused and politicized, the capability of altering video and photographs to use as evidence are becoming more convincing and will present challenges for even the most literate of the digital age.

The First Amendment's protection of the freedom of speech will permit certain types of disinformation and propaganda to be disseminated. If the consumer is educated on how to spot disinformation and evaluating sources beyond the superficial amount of likes and shares, the potential impact or influence of the disinformation can be lessened. The cyber-attack on Estonia in 2007 highlighted the vulnerability of liberal democratic systems that depend on the free flow of information.[7] The report also highlights the role that media has in holding politicians and others to account, but the media must maintain the trust of the people, or the populace will look for other sources of news and information, making them further susceptible to malign sources.[8]

The third prong of the strategy relies on the collaboration of the government and private sector. The government does not have the capability to restrict content on social media without restricting freedoms. Big tech companies do not have the "geopolitical cognition" of the United States' policy goals and are not focused on the social and political implications of the content.[9] The strengths of both need to be used for mutual benefit. A recent North American Treaty Organization's Strategic Communication report on social media manipulation gives four recommendations:

[6] Mad Scientist Laboratory, number 277
[7] 2007 Cyber Attacks on Estonia, NATO, 14.
[8] 2007 Cyber Attacks on Estonia, NATO, 14.
[9] Mad Scientist Laboratory, number 277.

1. Increase transparency and develop new safety standards for social media.
2. Establish independent and well-resourced oversight of social media.
3. Increase efforts to deter social media manipulation.
4. Continue to pressure social media platforms to do more to counter abuse of information.

NATO's recommendations put pressure on social media companies to police themselves without involvement or oversight from the government. The report highlights blocking the creation and use of fake or inauthentic accounts as the most important step social media platforms can take to stop manipulation.[10] The legislative branch of the US government can enact laws to discourage financial service providers from paying for the manipulation campaigns and pass legislation to punish those influencers or advertisers that utilize social media manipulation.[11]

While the social media companies are attempting to step up enforcement of fake accounts, the Federal Government can utilize agencies like the National Cyber Investigative Joint Task Force and the FBI's cyber watch center, Cywatch, to coordinate not only across government agencies but with the civilian sector. The FBI has the authority to coordinate with domestic law enforcement from national cyber intrusions.[12] The authority over national level threats can be utilized to contest the information

[10] Sebastian Bay, Anton Dek, Iryna Dek, and Rolf Fredheim, "Social Media Manipulation 2020: How Social Media Companies are Failing to Combat Inauthentic Behavior Online." NATO Strategic Communications Centre of Excellence, Nov 2020, 18.

[11] Bay, "Social Media Manipulation 2020: How Social Media Companies are Failing to Combat Inauthentic Behavior Online," 40.

[12] Congressional Research Service, Justice Department's Role in Cyber Incident Response, by Kristin Finklea, December 18, 2020.

environment during civil unrest in order to assist local law enforcement. And the military can legally assist when there is a shortage of resources or personnel.

There are other techniques that governments use to attempt to control social media during unrest. Internet blackouts are common in countries that have more authoritarian governments.[13] India uses rolling blackouts and throttling, which is reducing the bandwidth or speed of the internet.[14] However, when India used the techniques, it did see a negative impact on the economy.[15] In the race to establish the narrative, throttling in areas of unrest would give the USG some time to gather the facts or time for traditional media sources to check the authenticity of the story. However, the tendency for the truth to be lost in the sea of disinformation would still exist and the negative public reaction to the infringement of freedoms would offset any gains that could be had by blackouts or throttling.

In a scenario like the 2016 Presidential Election, USNORTHCOM would have the authorities to coordinate with law enforcement against cyber activities, conduct approved strategic communications, and utilize military means and personnel to assist in contesting disinformation and propaganda. The US citizens would have been exposed to digital media education through USG programs to lessen the effect of disinformation and propaganda as an ongoing campaign. Once the threat of a disinformation campaign is detected, social media companies would notify law enforcement through a federal agency like a USNORTHCOM Joint Task Force or FBI watch center. Social media companies would use existing policies of flagging disinformation. A definitive framework and

[13] Singer, *Like Wars,* 88.
[14] Singer, *Like Wars*, 89.
[15] Singer, *Like Wars ,* 89.

transparent standards for what should be reported to the JTF would have to be agreed upon or passed as legislation. Law enforcement would actively contest the campaign through cyber means or would request additional help from military assets in order to lessen the influence of the propaganda and begin attribution. In the event a riot or unlawful assembly is declared by local law enforcement or the local governments, the JTF would request permission to use geographic fencing for social media activity to assist law enforcement in the lessening of the severity of the civil unrest. The JTF would assist law enforcement in gathering information and potentially using military means to gather surveillance video to combat propaganda that uses selective video clips to foment more violence. The JTF would disseminate strategic communications of the involvement of the JTF, when classification permits, and contest the disinformation campaigns and propaganda being broadcast through cyber means.

The military has the authority through Title 10 of the US Code to be used by law enforcement in a passive role that augments and assists law enforcement. The Posse Comitatus Act would not be relevant to the passive military assistance being provided to law enforcement and the decision to use military capabilities would rest with law enforcement requesting assistance rather than state officials that may be looking at political ramifications in the request for federal assistance. The potential ramifications of the perception of limiting freedoms reduces the will of civilian leadership to confront or contest activities in the information environment. The use of military personnel and capabilities would be expanded to combat and contextualize malign activities attributed to a foreign entity with USNORTHCOM having additional authorities under Defense of the Homeland. Unity of command, understanding of the mission, and application of

Rules of Engagement (ROE) are additional attributes that make military forces value added to lessening the severity of violence in cooperation with law enforcement.[16] The unity of command under USNORTHCOM would simplify who is responsible for contesting the actions in the Information Environment when the threats blur the line between foreign and domestic security. The ROE would remain the same, instead of varying and potentially causing confusion as the issue transitions between federal agencies.

The main objective of contesting Operations in the Information Environment is to prevent or lessen the severity of civil unrest and riots. If the influence of disinformation campaigns and propaganda can be lessened prior to civil unrest turning violent, the use of military forces being employed under the Insurrection Act should be reduced. The cooperation between private corporations and law enforcement agencies is crucial in the detection of disinformation campaigns and the protection of civil liberties of the US citizens. First Amendment rights cannot be infringed by frivolous law enforcement techniques. If the propaganda and disinformation campaigns are being used against the United States, especially from foreign entities, the USG has a responsibility to contest malign actor's Operations in the Information Environment. Due process must be followed within the legal limits of law enforcement and the definition of propaganda and disinformation must be defined in an apolitical environment on the bedrock of the Constitution.

[16] Marvin L. Covault, *Should Federal Military Forces be Engaged in a National Civil Disturbance Crisis?,* https://wethepeoplespeaking.com/2020/06/04/should-federal-military-forces-be-engaged-in-a-national-civil-disturbance-crisis/.

Bibliography

Anonymous. "Understanding Media and Culture: An Introduction to Mass Communication." University of Minnesota, 2016.

Armstrong, Matt. "A Brief History of the Smith-Mundt Act and Why changing it matters." MountainRunner. Us (blog). Feb 23,2012. https://mountainrunner.us/2012/02/history_of_smith-mundt/.

Baker, Bonnie. The Origins of the Posse Comitatus. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/baker1.pdf.

Babbage, Ross. "Winning Without Fighting: Chinese and Russian Political Warfare Campaigns and How the West Can Prevail," Center for the Strategic and Budgetary Assessments, July 24,2019, https://csbaonline.org/research/publications/winning-without-fighting-chinese-and-russian-political-warfare-campaigns-and-how-the-west-can-prevail/publication/1.

Office of the Director of National Intelligence. *Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution.* Office of the Director of National Intelligence. January 6, 2017.

Bay, Sebastian, Anton Dek, Iryna Dek, and Rolf Fredheim, "Social Media Manipulation 2020: How Social Media Companies are Failing to Combat Inauthentic Behavior Online." NATO Strategic Communications Centre of Excellence, Nov 2020.

Congressional Research Service, *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*, by Kristin Finklea and Catherine A. Theohary. January 15, 2015.

Congressional Research Service, *Information Warfare: Issues for Congress,* by Catherine A. Theohary, March 5, 2018.

Congressional Research Service, *The Posse Comitatus Act and Related Matters: The Use of the Military to Execute Civilian Law,* by Jennifer K. Elsea. November 6, 2018.

Congressional Research Service, *Justice Department's Role in Cyber Incident Response*, by Kristin Finklea, December 18, 2020.

Congressional Research Service, *Election Security: Issues in the 2018 Midterm Elections,* by Catherine Theohary and Eric Fischer, August 16, 2018.

Cornell Law School. "Military Power in Law Enforcement: The Posse Comitatus." https://www.law.cornell.edu/constitution-conan/article-2/section-3/military-power-in-law-enforcement-the-posse-comitatus.

Denton, Allison. Fake News: The Legality of the Russian 2016 Facebook Influence Campaign. *Boston University International Law Journal* 37, no. 183(April 2019): 183-210.

Domestic Operational Law Handbook 2018 for Judge Advocates. Center for Law and Military Operations, 2018.

Hollis, Duncan B., "Why States Need An International Law for Information Operations," Lewis and Clark Law School, December 5, 2007, https://law.lclark.edu/live/files/9551-lcb114art7hollis.pdf.

Information Operations. *Joint Publication 3-13*. Joint Chiefs of Staff Washington DC, 2014.

Jamieson, Kathleen Hall. How Russian Hackers and Trolls Exploited U.S. Media in 2016. *Proceedings of the American Philosophical Society* 163, no. 2 (June 2019) 122-135.

Joes, Anthony James, Victorious Insurgencies: Four Rebellions the Shaped Our World (Lexington, KY: University Press of Kentucky, 2010).

Kahn, Matthew. "DHS Cybersecurity Strategy," Lawfare, May 17, 2018, https://www.lawfareblog.com/document-dhs-cybersecurity-strategy.

Lapowsky, Issie and Steven Levy. "Here's What Facebook Won't Let You Post." WIRED. Apr 24, 2018. https://www.wired.com/story/heres-what-facebook-wont-let-you-post/.

Larson, Eric V. and John E. Peters, Preparing the U.S. Army for Homeland Security: Concepts, Issues, and Options. Santa Monica, CA: RAND Corporation, 2001. https://www.rand.org/pubs/monograph_reports/MR1251.html.

Lawfare Podcast. "Alex Stamos on the Hard Tradeoffs of the Internet." Produced by Jen Patja Howell. February 13,2020. https://www.lawfareblog.com/lawfare-podcast-alex-stamos-hard-tradeoffs-internet.

Lin, Herb. "Doctrinal Confusion and Cultural Dysfunction in the Pentagon Over Information and Cyber Operations" Lawfare, March 27, 2020. https://www.lawfareblog.com/doctrinal-confusion-and-cultural-dysfunction-pentagon-over-information-and-cyber-operations.

Schlichter, Kurt Andrew. "Locked and Loaded: Taking Aim at the Growing Use of the American Military in Law Enforcement Operations," Loyola of Los Angeles Law Review 26, no. 4 (June 1993): 1291-1334.

Singer, P.W., and Emerson T. Brooking. *Like War: The Weaponization of Social Media.* New York, New York: Houghton Mifflin Harcourt Publishing Company, 2018.

US Army Mad Scientist Blog. "Insights from the Mad Scientist Weaponized Information Series of Virtual Events." October 19, 2020.

https://madsciblog.tradoc.army.mil/277-insights-from-the-mad-scientist-weaponized-information-series-of-virtual-events/.

US Constitution, Bill of Rights Amendment I.

US Department of Defense, Office of General Counsel. *Department of Defense Law of War Manual*, by Stephen W. Preston, June 2015.

US Department of Defense, Office of the General Counsel, *An Assessment of International Legal Issues in Information Operations,* by Philip A. Johnson, May 1999. https://fas.org/irp/eprint/io-legal.pdf.

Zabrisky, Zarina. "Big Lies and Rotten Herrings: 17 Kremlin Disinformation Techniques you need to know" Byline Times, March 04,2020, https://bylinetimes.com/2020/03/04/big-lies-and-rotten-herrings-17-kremlin-disinformation-techniques-you-need-to-know-now/.

Vita

CDR Ben “Tiny” Hartman’s most recent assignment was the GLOBAL THUNDER team chief assigned to US STRATEGIC COMMAND J7 in Omaha, Nebraska. He was responsible for the planning and execution of STRATCOM’s primary Tier 1 exercise. He was also a Strike Advisor and assisted with the training of the nuclear command and control enterprise. CDR Hartman entered the Navy in 2002 and was commissioned through Officer Candidate School in Pensacola, FL. He was winged as a Naval Flight Officer in 2004. He has served in 4 Electronic Attack squadrons and has been qualified in the EA-6B Prowler and the EA-18G Growler. CDR Hartman has been on multiple deployments supporting OPERATION ENDURING FREEDOM and OPERATION IRAQI FREEDOM. CDR Hartman received a Bachelor of Science in Political Science from the University of Dubuque and a Master's degree from the Naval War College.