National Security Law Journal

VOLUME 4

ISSUE 1

FALL/WINTER 2015

National Security Law Journal
George Mason University School of Law
3301 Fairfax Drive
Arlington, VA 22201

www.nslj.org

Library of Congress Publication Data (Serial)

National Security Law Journal. Arlington, Va. : National Security Law Journal, 2013-
K14 .N18
ISSN: 2373-8464
Variant title: NSLJ
National security—Law and legislation—Periodicals
LC control no. 2014202997 (http://lccn.loc.gov/2014202997)

Past issues available in print at the Law Library Reading Room of the Library of Congress (Madison, LM201).

VOLUME 4, ISSUE 1 (FALL/WINTER 2015)
ISBN-13: 978-1523203987
ISBN-10: 1523203986

National Security Law Journal

ARTICLES

COMMENTS

VOLUME 4 FALL/WINTER 2015 ISSUE 1

NATIONAL SECURITY
LAW JOURNAL

PUBLISHED BY GEORGE MASON UNIVERSITY SCHOOL OF LAW

Cite as 4 NAT'L SEC. L.J. ___ (2015).

The *National Security Law Journal* ("NSLJ") is a student-edited legal periodical published twice annually at George Mason University School of Law in Arlington, Virginia. We print timely, insightful scholarship on pressing matters that further the dynamic field of national security law, including topics relating to foreign affairs, homeland security, intelligence, and national defense.

Visit our website at www.nslj.org to read our issues online, purchase the print edition, submit an article, learn about our upcoming events, or sign up for our e-mail newsletter.

The Editors of NSLJ can be contacted at:

National Security Law Journal
George Mason University School of Law
3301 Fairfax Drive
Arlington, VA 22201

Publications: Our print edition is available from retail bookstores, including Amazon and Barnes & Noble. Digital versions of our full issues are available on our website, www.nslj.org.

Submissions: We welcome submissions from all points of view written by practitioners in the legal community and those in academia. We publish articles, essays, and book reviews that represent diverse ideas and make significant, original contributions to the evolving field of national security law. For more information, please visit www.nslj.org/submissions/.

Articles, manuscripts, and other editorial correspondence should be addressed to the NSLJ Articles Selection Editor at the mailing address above or by e-mail to submissions@nslj.org.

NATIONAL SECURITY
LAW JOURNAL

VOLUME 4 | FALL/WINTER 2015 | ISSUE 1

2015-2016 EDITORIAL BOARD

NATIONAL SECURITY
LAW JOURNAL

PUBLISHED BY GEORGE MASON UNIVERSITY SCHOOL OF LAW

FOREWORD

This issue marks the beginning of our fourth volume. The journal continues to grow at a rapid pace as evidenced by our largest Candidate Member class to date. Our success is possible because of our many dedicated readers and supporters.

In this issue, Major Patrick Walsh, Associate Law Professor at the Army's Judge Advocate General's School, analyzes a framework where national security professionals can predict changes to the Foreign Intelligence Surveillance Act to determine which programs are at risk of removal by future executive, legislative or judicial action; and Jesse Medlong, an Associate at DLA Piper LLP (US), uses quantum theory to examine the unique legal role of delegated authority and standard operating procedures in the military. This issue also contains two comments by Mason students: Stephen Jackson proposes designating Mexican drug cartels as foreign terrorist organizations to facilitate prosecution, and Molly Picard examines potential civil liabilities for U.S. military personnel engaged in the cyberspace battlefield.

I invite you to connect with us on social media via Facebook (facebook.com/NatlSecLJ), on Twitter (@NatlSecLJ), and on our YouTube channel (youtube.com/NatlSecLJ). I hope you enjoy this issue and that you will join the conversation so that we can continue our exploration in the dynamic field of national security law.

Rick Myers
Editor-in-Chief

National Security
Law Journal

VOLUME 4 FALL/WINTER 2015 ISSUE 1

Contents

ARTICLES

COMMENTS

PLANNING FOR CHANGE:
BUILDING A FRAMEWORK TO PREDICT FUTURE CHANGES TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

Patrick Walsh*

In the last several years, the United States has begun to scrutinize the expansive surveillance powers that were enacted after September 11, 2001. Intelligence surveillance programs previously considered lawful and reliable ways to gather information are being rescinded by Congress, declared unlawful by the courts and restricted by the executive branch. In an era of increasing scrutiny on the intelligence community, national security professionals must look beyond the statutory authorization for intelligence gathering, and evaluate each intelligence program to determine if it will endure past current efforts to restrict government surveillance powers. This article will develop a framework to analyze our current intelligence gathering programs and determine which programs are at risk of removal by future executive, legislative or judicial action.

By examining the historical struggle between the intelligence community's need for broad powers to protect the nation from foreign enemies and our nation's strong commitment to protecting the civil liberties of citizens from government intrusion, a national security lawyer can determine how our nation has expanded, modified, restricted, and rescinded other intelligence gathering programs to meet the nation's national security goals. Comparing

* Associate Professor, International and Operational Law Department, The Judge Advocate General's School, United States Army, Charlottesville, Virginia. J.D., 1998, University of California at Berkeley; L.L.M., 2009, The Judge Advocate General's School, United States Army, Charlottesville, Virginia; L.L.M. (candidate) 2016, University of Virginia Law School. The author is a military reservist currently serving on active duty. In his civilian life, he is an Assistant United States Attorney who handles national security cases for the U.S. Attorney's Office in the District of Nevada.

the history and development with a modern look at how the public and the government have responded to current surveillance powers will illustrate the factors that create an increased risk for an intelligence program to be weakened or eliminated by judicial, legislative, or executive action. Using this framework, a cautious national security professional can carefully decide which of the currently available intelligence collection options are likely to both meet the current collection requirements and also endure the current increased scrutiny on surveillance. The Foreign Intelligence Surveillance Act ("FISA") will change again, and national security professionals must be prepared for these changes.

INTRODUCTION

The foreign intelligence surveillance framework has been modified significantly since the terrorist attacks of September 11,

2001.[1] Expansive surveillance powers were granted to the intelligence and law enforcement communities in order to protect the nation from future attacks.[2] A decade later, the validity of these same programs is being reexamined.[3] Foreign intelligence surveillance programs that were once considered lawful and reliable ways to gather information are being rescinded by Congress, declared unlawful by the courts, and restricted by the executive branch.[4] As a result, national security professionals in charge of gathering intelligence information and using it to protect the nation must reassess the information they have gathered and determine what to do with it. Officials wishing to use the intelligence as evidence in a criminal case must determine whether it is still admissible, even if the methods were lawful when the government first acquired the intelligence.[5] In addition to these considerations for gathering intelligence and prosecuting individuals, the intelligence community must reevaluate all of the remaining intelligence gathering programs to determine which programs Congress or the judiciary are more likely to remove, and which programs will remain available for future use.

In an era of increasing scrutiny on the intelligence community, national security professionals must look beyond the

---

[1] *See, e.g.*, The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56 § 218, 115 Stat. 272, 291 (codified at 50 U.S.C. § 1804(a)(6)(B) (2006)); FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2463, 2473 (2008).

[2] 50 U.S.C. § 1804(a)(6)(B); 122 Stat. at 2473.

[3] *See, e.g.*, ACLU v. Clapper, 785 F.3d 787, 810 (2d Cir. 2015) (holding that the Section 215 Program did not preclude judicial review); United States v. Mohamud, No. 3:10–CR–00475–KI–1, 2014 WL 2866749, at *26 (D. Or. June 24, 2014); PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 86–97 (2014), https://www.pclob.gov/library/702-Report.pdf (detailing the PCLOB's review of the Fourth Amendment issues raised by the surveillance program operated under Section 702).

[4] *See* Memorandum from Jamie S. Gorelick, Deputy Att'y Gen., to Mary Jo White, U.S. Att'y, S. Dist. N.Y. et al. 1, https://fas.org/irp/ agency/doj/1995_wall.pdf [hereinafter Gorelick Memo]; *see also* Memorandum from Janet Reno, Att'y Gen., to Assistant Att'y Gen. et al. § (A)(6) (July 19, 1995), http:// www.fas.org/irp/agency/ doj/fisa/1995procs.html [hereinafter Reno Memo].

[5] *See Clapper*, 785 F.3d at 813; Issuance of Order, 50 U.S.C. § 1805 (2012).

statutory authorization for intelligence gathering and evaluate each intelligence program for the likelihood that the Court will revoke it, Congress will rescind it, or the executive branch will restrict it. This article will discuss an approach to scrutinize our current intelligence gathering and determine which programs are at risk to be removed by future executive, legislative, or judicial action.

This article begins its analysis in Part I, with an examination of the historical struggle between the intelligence community's need for broad powers to protect the nation from foreign enemies, and our nation's strong commitment to protecting the civil liberties of citizens from government intrusion. Understanding the development of this debate, which led to the Foreign Intelligence Surveillance Act ("FISA"),[6] gives context to how our nation has expanded, modified, restricted, and rescinded other intelligence gathering programs to meet the nation's national security goals. Intelligence professionals who are familiar with the genesis of the current intelligence gathering systems will be more adept at assessing which programs may disappear. Next, Part II will introduce FISA, and provide a brief explanation of how it works, and how it restricted sharing between the intelligence and law enforcement communities before the September 11, 2001, attacks. Part III examines the amendments to FISA after the September 11th attacks that expanded the ability to gather foreign intelligence and removed barriers to information sharing. It concludes with a look at how the public and the government have responded to these new expansive surveillance powers. Finally, Part IV analyzes the factors that create an increased risk for an intelligence program to be weakened or eliminated by judicial, legislative, or executive action.

I. THE BEGINNING OF THE INTELLIGENCE DEBATE—LIFE BEFORE FISA

The first decades of telephone wiretaps were without controversy, and the President conducted intelligence collection

[6] An Act to Authorize Electronic Surveillance to Obtain Foreign Intelligence Information, Pub. L. No. 95-511, 92 Stat. 1783 (1978).

without the involvement of other branches of government.[7] Telephone wiretaps during World War II were a prime example of national security intelligence collection without judicial approval.[8] Successive presidents expanded the use of these warrantless wiretaps to obtain national security and foreign intelligence information.[9] This policy continued until the 1960s with little concern or controversy from the legislative or judicial branches of government. However, that changed in the late 1960s when prosecutors attempted to use these wiretaps as evidence in criminal trials.[10]

*A. Pre-*Katz *Intelligence Gathering*

Prior to 1967, there was tacit judicial approval of all warrantless telephone surveillance.[11] In its 1927 decision in *Olmstead v. United States*, the Supreme Court held that telephone surveillance did not violate the Fourth Amendment because it did not constitute the requisite physical trespass.[12] Although this created the possibility of unrestrained government telephone surveillance, the executive and legislative branches later reduced that risk by prohibiting the use of wiretaps as evidence in court proceedings.[13] This created a civil liberties "compromise" where government agents

---

[7] Zweibon v. Mitchell, 516 F.2d 594, 674 (D.C. Cir. 1975) (Appendix A: Memorandum from President Franklin D. Roosevelt to Attorney General Robert Jackson); *see also* Herbert Brownell, Jr., *The Public Security and Wire Tapping*, 39 CORNELL L.Q. 195, 197-98 (1954).

[8] *Zweibon*, 516 F.2d at 674; *see also* Brownell, *supra* note 7, at 199-200.

[9] Memorandum from Att'y Gen. Herbert Brownell for J. Edgar Hoover, FBI Dir. 296-97 (May 20, 1954), *reprinted in* FRANK CHURCH ET AL., INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK 2, S. REP. NO. 94-755, at 296-97 (1976), http://www.intelligence.senate.gov/sites/default/files/94755_III.pdf; Memorandum from Att'y Gen. Nicholas Katzenbach for J. Edgar Hoover, FBI Dir. (Sept. 27, 1965), *reprinted in* S. REP. NO. 94-755, at 287; Press Release, U.S. Dep't of Justice (Sept. 12, 1973), *reprinted in* L. Rush Atkinson, *The Fourth Amendment's National Security Exception: Its History and Limits*, 66 VAND. L. REV. 1343, 1383 (2013).

[10] Katz v. United States, 389 U.S. 347, 353 (1967).

[11] Olmstead v. United States, 277 U.S. 438, 468-69 (1928).

[12] *Id.* at 466 (holding that there was no reasonable expectation of privacy because the bug was placed on the wire in a public area).

[13] *See* Nardone v. United States, 302 U.S. 379, 381 (1937); *see also* Radio Act of 1927, Pub. L. No. 632, § 27, 44 Stat. 1162, 1172 (1927); *see also* Department of Justice Appropriations Act of March 1, 1933, Pub. L. No. 387, 47 Stat. 1371, 1381 (1933).

had few limitations on their ability to use wiretaps, but little incentive to do so for anything other than to gather foreign intelligence.[14] Some began to see this compromise as a "national security exception" to the Fourth Amendment's warrant requirement—which permitted the use of national security wiretaps without a warrant, but prohibited the government from introducing any of this intelligence at trial.[15]

B. Katz *and Search Warrants for Wiretaps*

The Supreme Court again reviewed the lawfulness of warrantless wiretapping in *Katz v. United States*. Decided in 1967, *Katz* brought wiretaps under the protection of the Fourth Amendment while leaving open the possibility that certain circumstances could allow for national security wiretaps without a search warrant.[16] In *Katz*, the Supreme Court determined that Federal Bureau of Investigation ("FBI") Agents violated the Fourth Amendment when they obtained a telephone wiretap without first seeking a judicially authorized warrant.[17] Even though the wiretap did not involve a trespass, the Court held that it nonetheless constituted a Fourth Amendment "search" and was unconstitutional unless the agents obtained a judicially authorized search warrant to conduct the wiretap.[18] The Court further held that searches without judicially authorized search warrants "are per se unreasonable under the Fourth Amendment."[19] Courts have routinely followed the

[14] *Nardone*, 302 U.S. at 381. If it was inadmissible in court, it would not be useful in criminal investigations. Therefore, it would be primarily used only by those who gathered information for its intelligence value.
[15] *Katz*, 389 U.S. at 358 n.23; *see* Atkinson, *supra* note 9, at 1356 (explaining the detailed history of the origins and limits of the national security exception).
[16] *Katz*, 389 U.S. at 353 (reversing *Olmstead*).
[17] *Id.*
[18] *Id.* The Supreme Court overruled its prior decision in *Olmstead* when it determined that the Fourth Amendment can be violated without a physical trespass. *Id.*
[19] *Id.* at 357.

principle that searches without warrants carry a presumption of unreasonableness unless they fit into a narrow group of exceptions.[20]

Katz involved a wiretap for a criminal investigation into illegal gambling with no national security implications.[21] Nonetheless, the Court addressed national security wiretaps through dicta in its well-known footnote 23.[22] This footnote specifically raised the question of "[w]hether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving national security,"[23] but did not provide an answer, as the "question was not presented by this case."[24] Footnote 23 suggested the possibility that agents could conduct national security and foreign intelligence searches without obtaining a search warrant.[25]

Katz left a ray of hope for national security cases.[26] *Katz* was a criminal case with no national security or intelligence nexus, and the Court left open the possibility that agents could conduct national security and foreign intelligence searches without obtaining a search

[20] *Id.*; *see, e.g.*, Warden v. Hayden, 387 U.S. 294, 298-300 (1967) (police may conduct an investigation if delay in obtaining a warrant would gravely endanger their lives or the lives of others); Cooper v. California, 386 U.S. 58, 87 (1967) (warrantless search of a seized automobile is proper if the search is directly related to why defendant was arrested); Brinegar v. United States, 338 U.S. 160, 174-77 (1949) (searches and seizures resulting from a police mistake may be permissible without a warrant if the mistake is reasonable); McDonald v. United States, 335 U.S. 451, 454-56 (1948) (police may conduct a search without a warrant when there are exigent or emergent circumstances, but inconvenience to the police officers and delay in preparing a warrant are not compelling reasons to justify a search without a warrant); Carroll v. United States, 267 U.S. 132, 153, 156 (1925) (police may search an automobile without a warrant if they have probable cause to believe evidence is located in the automobile).

[21] *Katz*, 389 U.S. at 354.

[22] *Id.* at 358 n.23 (planting the seed for the modern national security exception to the Fourth Amendment's warrant requirement thus becoming a well-known footnote (or exception?) in the national security arena).

[23] *Id.*

[24] *Id.*; *see* Stephanie Cooper Blum, *What Really is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform*, 18 B.U. PUB. INT. L.J. 269, 273–74 (2009).

[25] *Katz*, 389 U.S. at 358 n.23.

[26] *Id.*; *see* Blum, *supra* note 24, at 273-74.

warrant.[27] The Court's language implicitly invited Congress to create a legislative framework for the application and approval of criminal wiretaps.[28] Because *Katz* did not explicitly hold on national security and foreign searches, law enforcement who sought to turn foreign intelligence into evidence for use in criminal prosecutions were left unsure whether their national security wiretaps obtained without a search warrant were lawful.

C. *Legislative Response to* Katz*, and Lead Up to FISA*

Congress responded to the Court's holding through the enactment of a broad framework for criminal wiretaps in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (commonly referred to as "Title III").[29] However, Title III addressed only criminal wiretaps and left open the possibility that intelligence searches did not require a Title III judicially authorized warrant.[30] In vague language, Congress suggested that the President might have constitutional power to authorize intelligence searches without seeking judicial approval for cases involving national security.[31] Congress stated that Title III was not intended to "limit the constitutional power of the President . . . to protect the Nation against actual or potential attack,"[32] or "to obtain foreign intelligence information"[33] or "to protect the United States against any clear and present danger to the structure or existence of the Government."[34] One could also read this language much more narrowly however, to suggest that Congress did not agree that the President had such authority but was not trying to resolve that issue in this legislation.[35]

---

[27] *Katz*, 389 U.S. at 358 n.23.
[28] *Id.* (suggesting Congress could create "safeguards other than prior authorization by a magistrate" that could "satisfy the Fourth Amendment in a situation involving the national security").
[29] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197 (1968).
[30] *Id.* at §801(c); Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. I, at § 101(b)(3).
[31] Pub. L. No. 90-351, tit. I, at § 101(b)(3).
[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *See id.*; *see also* Atkinson, *supra* note 9, at 1397.

The executive branch took the former, more expansive view, and continued to conduct national security wiretaps without judicial oversight or approval.[36]

The issue was brought to the Court's attention four years later, with a case involving the bombing of a Central Intelligence Agency Office in Ann Arbor, Michigan.[37] In *United States v. United States District Court* (now called the *Keith* case), the Supreme Court found that a warrantless national security wiretap conducted inside the United States violated the Fourth Amendment.[38] The fact that it was labeled a national security case did not make the warrantless surveillance lawful.[39] Once again, the Supreme Court did not clarify the scope of its decision to require warrants in national security cases.[40] The Court clearly held that search warrants are required for domestic national security cases.[41] However, the Court left open the possibility that warrantless wiretaps for extraterritorial national security cases may be lawful.[42]

Keith marked the beginning of increased concern and growing restrictions on the ability of intelligence professionals to collect and share national security information. But the executive branch did not heed the concerns expressed in *Keith*, and continued to gather intelligence information (or more precisely, information

[36] *See* Atkinson, *supra* note 9, at 1397 (the executive branch continued to authorize wiretaps without a warrant for national security purposes).
[37] United States v. U.S. District Court (*Keith*), 407 U.S. 297, 299 (1972) (known as the *Keith* case after Judge Keith, who wrote the lower court opinion); *see* Atkinson, *supra* note 9, at 1381 (detailing the history of the origins and limits of the national security exception). Others have referred to this more generally as a "special needs" exception. *See* Owen Fiss, *Even in a Time of Terror*, 31 YALE L. AND POL'Y REV. 1, 25–27 (2012). This paper uses the phrase national security exception because it is more specific to the present topic.
[38] *Keith*, 407 U.S. at 299-300, 318.
[39] *Id.*
[40] *Id.* at 324.
[41] *Id.* The Court softened its holding by limiting the warrant requirement to the facts of this case, and also invited Congress to propose "reasonable standards" that may apply in domestic national security searches. *Id.*
[42] *Id.* at 323-24.

claimed to be for intelligence) without obtaining a search warrant.[43] Congress took notice of the executive's warrantless wiretapping and began to view the efforts to gather intelligence as overreaching and abusive.[44] As a result, Congress acted to investigate and eventually curb these perceived executive branch abuses of intelligence tools.[45]

II. FISA—THE BUILDING OF A WALL

The Watergate scandal brought the concern of misuse of the intelligence apparatus by the executive branch to the forefront of the national consciousness.[46] The United States Senate responded by setting up the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, more commonly known as the Church Committee.[47] The Church Committee conducted many public hearings and published a detailed report citing numerous abuses of the executive branch, including cloaking warrantless surveillance of political dissidents and opponents under the guise of "national security."[48] These misdeeds extended to both the military and FBI, and they occurred in the Nixon administration as well as previous administrations.[49] To fix these abuses, Congress sought to create a comprehensive statutory framework requiring the executive branch to regulate intelligence collection within the United States.[50]

---

[43] *See* Charles R. Nesson, *Aspects of the Executive's Power Over National Security Matters: Secrecy Classifications and Foreign Intelligence Wiretaps*, 49 IND. L.J. 399, 412-13 (1974).

[44] Michael P. O'Connor & Celia Rumann, *Going, Going, Gone: Sealing the Fate of the Fourth Amendment*, 26 FORDHAM INT'L L.J. 1234, 1255 (2003); *see also* FRANK CHURCH ET AL., INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK 2, S. REP. NO. 94-755, at 2-3 (1976).

[45] *See* CHURCH ET AL., *supra* note 44, at 2-3.

[46] *See* O'Connor & Rumann, *supra* note 43, at 1255.

[47] *See* CHURCH ET AL., *supra* note 44, at 4-5; *see generally* O'Connor & Rumann, *supra* note 44, at 1255.

[48] *See* Evan Tsen Lee, *The Legality of the NSA Wiretapping Program*, 12 TEX. J.C.L. & C.R. 1, 38-39 n.142 (2006).

[49] *Id.* at 38; *see also* Michael German, *Trying Enemy Combatants in Civilian Courts*, 75 GEO. WASH. L. REV. 1421, 1432 (2007).

[50] 50 U.S.C. § 1802 (1978).

Congress passed FISA in 1978, in part as a response to government abuses of wiretaps and in part as an answer to the invitation of the *Keith* court to address the issue of national security wiretaps.[51] FISA served as a comprehensive statutory framework for the executive branch to obtain judicially sanctioned wiretaps, gather foreign intelligence, and provide for national security.[52] The statute made Congress's intent clear, that wiretaps for intelligence purposes required judicial authorization through the newly created Foreign Intelligence Surveillance Court ("FISC").[53] After *Katz*, Title III, *Keith* and FISA, there were clearly defined limits on the ability of the intelligence community to gather intelligence information, particularly domestic intelligence information.[54] Both Congress and the public remained concerned of abuses and government officials in all three branches began to restrict not just the ability to obtain intelligence information, but also the ability to share the information collected. These restrictions were designed to limit the sharing of intelligence information with law enforcement personnel.

A. How FISA Worked and How it Restricted Sharing

FISA created an alternate path for the government to obtain wiretaps and search warrants in foreign intelligence cases.[55] For intelligence professionals, FISA had advantages over Title III criminal wiretaps; the court operated in a classified setting, interceptions could last for a longer duration, and the monitoring procedures were more advantageous to the government.[56] These

---

[51] *See* William C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209, 1211, 1227 (2007).

[52] 50. U.S.C. § 1802. A detailed explanation of judicially authorized wiretaps under FISA is beyond the scope of this article, which will focus on the wiretaps conducted without a judicial warrant.

[53] *See* 50 U.S.C. §§ 1803, 1809(a)(1) (1978) (making it a crime to "engage in electronic surveillance . . . except as authorized by this Act."). A detailed explanation of judicially authorized wiretaps under FISA is beyond the scope of this article, which will focus on the wiretaps conducted without a judicial warrant.

[54] Katz v. United States, 389 U.S. 347, 358 n.23 (1967); United States v. U.S. District Court (*Keith*), 407 U.S. 297, 324 (1972); 50 U.S.C. § 1801(f) (2015).

[55] *See*, *e.g.*, 50 U.S.C. §§ 1802-1805 (2015) (detailing the process for the government to apply and get approved for electronic surveillance).

[56] *See* 50 U.S.C. §§ 1801(h), 1802(a) (2015 & 2010).

advantages raised the concern that the executive branch would use FISA as a way to circumvent the criminal court process in cases not involving foreign intelligence. Therefore, Congress wrote protections into the statute to ensure the government could only use the surveillance tools in FISA for gathering foreign intelligence.[57]

The statute required that "the purpose" of surveillance was to obtain "foreign intelligence information."[58] However, this language was subject to multiple reasonable interpretations.[59] What if the government wanted to obtain foreign intelligence information but also wanted to investigate a crime? Congress did not state whether "the purpose" meant the *only* pupose, the primary purpose or a significant purpose. The courts were left to resolve what "the purpose" means when the government is gathering foreign intelligence.[60]

Federal courts answered this question and took a very restrictive view of "the purpose" of FISA.[61] Every court to review the issue determined that "purpose" really meant "the *primary* purpose."[62] These courts reasoned that national security professionals seeking FISA authorization to wiretap an individual's

[57] 50 U.S.C. § 1804(a)(6)(B) (2010).
[58] *Id.* *See also* DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS, 2D, §10.3 Westlaw (database updated July 2015).
[59] *See* United States v. Truong Dinh Hung, 629 F.2d 908, 911 (4th Cir. 1980) (interpreting pre-FISA law and significantly influencing all subsequent cases); *In re* Sealed Case, 310 F.3d 717, 725 (FISA Ct. Rev. 2002) (discussing the development of the primary purpose test).
[60] 50 U.S.C. § 1804(a)(6)(B). *See also* KRIS & WILSON, *supra* note 58, at § 10.3.
[61] *See* KRIS & WILSON, *supra* note 58, at § 10.3; s*ee Truong Dinh Hung*, 629 F.2d at 915-16; *see also In re Sealed Case*, 310 F.3d at 725 (FISA Ct. Rev. 2002).
[62] *See* United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991), *overruled by* United States v. Abu-Jihaad, 630 F.3d 102, 126 (2d Cir. 2010) (overruling court still acknowledging the "primary purpose" of FISA to collect foreign intelligence); United States v. Pelton, 835 F.2d 1067, 1074-75 (4th Cir. 1987); United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987); United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984).

phone must establish that the primary purpose of the investigation is to gather foreign intelligence.[63]

The primary purpose test still left theoretical room for law enforcement officers to participate in intelligence investigations. As long as foreign intelligence gathering was the *primary* purpose, there could potentially be *secondary* purposes.[64] One of those secondary purposes could be law enforcement, but involving law enforcement in the investigation creates risk. A reviewing court might disagree and decide—after the fact—the primary purpose was really law enforcement and not foreign intelligence.[65] Alternatively, a reviewing court may agree that the primary purpose was *initially* to gather foreign intelligence, but during the course of the investigation, the primary purpose switched to a law enforcement purpose.[66] This can happen when investigators begin to determine that prosecution is warranted and continue to use FISA approved surveillance while developing a criminal case.

The risk that a court may disapprove of the "purpose" of the investigation raised concerns in the Department of Justice ("DOJ"). Although Federal courts assumed that the sharing of FISA derived information after the investigation ended was permissible, government lawyers added additional executive branch restrictions to mitigate this risk.[67] A cautious executive branch, perhaps

[63] *See Truong Dinh Hung*, 629 F.2d at 915-16; *In re Sealed Case*, 310 F.3d at 725. *See also Johnson*, 952 F.2d at 572; *Pelton*, 835 F.2d at 1074-75; *Badia*, 827 F.2d at 1464; *Duggan*, 743 F.2d at 77.

[64] Courts before September 11, 2001 had found that the foreign intelligence exception applied where the "primary purpose" was the gathering of foreign intelligence. *See* United States v. Truong Dinh Hung, 629 F.2d 908, 915 (4th Cir. 1980); United States v. Megahey, 553 F. Supp. 1180, 1189-90 (E.D.N.Y.1982), *aff'd sub nom.* United States v. Duggan, 743 F.2d 59 (2d Cir. 1984). *In re Directives* expanded the exception (for FISC purposes) to allow warrantless searches that met the lower "significant purpose" standard. *In re* Directives, 551 F.3d 1004, 1011 (FISA Ct. Rev. 2008).

[65] *See In re Sealed Case*, 310 F.3d at 725-26.

[66] *See id.* at 725-27.

[67] *Id.*

chastened by the past abuses, placed additional policy restrictions on the sharing of intelligence information.[68]

B. The Department of Justice and Its Restrictions on Access to Foreign Intelligence Information

The DOJ attorneys created policy restrictions on the sharing of intelligence information with law enforcement. These restrictions alleviated some of the risk of post facto judicial review of the "primary purpose" of the investigation.[69] After examining the relevant judicial opinions and the approving statements of the Congressional committees that oversee FISA cases, the DOJ added additional regulations to ensure that all intelligence investigations complied with the primary purpose test.[70] These procedures—and their implementation—made it nearly impossible to share intelligence information with law enforcement officials.[71]

The intent of the procedures was to separate counterintelligence investigations from criminal investigations and to prevent any appearance that the federal government was using the intelligence tools for the primary purpose of furthering a criminal investigation.[72] These restrictions created what one court later called a "wall" to prevent the FBI intelligence officials from communicating with the Criminal Division regarding intelligence investigations.[73] These restrictions that limited sharing intelligence information with law enforcement were in effect on September 11, 2001, and may have contributed to the failure to identify and locate the 9/11 hijackers and, perhaps, stop the September 11 attacks.[74] After the

---

[68] *See* Gorelick Memo, *supra* note 4, at 2-4; *see also* Reno Memo, *supra* note 4, at § (A)(6).
[69] *See* SELECT COMM. ON INTELLIGENCE, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978: THE FIRST FIVE YEARS, S. Rep. No. 660-98, at 14 (1984).
[70] *Id.* at 15.
[71] NAT'L COMM. ON TERRORIST ATTACKS, THE 9/11 COMMISSION REPORT: FINAL REPORT ON THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, 271 (2004) [hereinafter THE 9/11 COMMISSION REPORT].
[72] Gorelick Memo, *supra* note 4, at 2-3.
[73] *See In re* Sealed Case, 310 F.3d 717, 728 (2002).
[74] THE 9/11 COMMISSION REPORT, *supra* note 71, at 271-72, 277 (noting "deep institutional failings within the government" including (1) a decrease in FISA

September 11, 2001, attacks, Congress amended FISA to eliminate the restrictions imposed by the judicial and executive branches, and began to expand the tools available to the intelligence community to address the threat of terrorism.[75]

III. THE COUNTRY'S ABOUT-FACE: EMPOWERING LAW ENFORCEMENT TO USE FISA

After the attacks of September 11, 2001, the executive and legislative branches realized that the restrictions placed on the intelligence tools from 1968 to 2001 created a system ill fitted to protect the nation from contemporary threats.[76] Both Congress and the President took actions to remove these long-standing restrictions, and created new and broader tools to aid in the collection and sharing of intelligence with law enforcement. Some of these broad intelligence collection programs expanded authorities within FISA.[77]

A. Removing Restrictions and Adding New Authorities to FISA

Congress dismantled the wall that courts erected around the primary purpose requirement in FISA.[78] Courts had previously read into FISA a requirement that the "primary purpose" of FISA surveillance must be to gather foreign intelligence.[79] Congress eliminated this requirement by changing the text from "the purpose" to a "significant purpose."[80] Congress added the word "significant" to destroy the executive created wall, which had restricted the sharing of intelligence with law enforcement, and to encourage information

applications leading up to the attacks, (2) some of the FISA wiretaps were discontinued before September 11, 2001, and (3) there was a misunderstanding about the ability to share FISA information on one of the 9/11 hijackers that prevented investigators from taking action that "could have derailed" the 9/11 attacks).

[75] Pub. L. 261-261, 122 Stat. 2463, 2473 (2008).

[76] THE 9/11 COMMISSION REPORT, *supra* note 71, at 277.

[77] *See id.*; 122 Stat. at 2473.

[78] 50 U.S.C. § 1804(a)(6)(B) (2012).

[79] *See* United States v. Truong Dinh Hung, 629 F.2d 908, 915 (4th Cir. 1980); United States v. Duggan, 743 F.2d 59 (2d Cir. 1984).

[80] *See* 50 U.S.C. § 1804(a)(6)(B) (2012).

sharing.[81] Under the revised law, FISA tools could be used even if there was a law enforcement purpose to the investigation.[82] The intelligence community was now strongly encouraged to share relevant information with law enforcement.

Congress took additional steps to increase the gathering of foreign intelligence. From President Bush's warrantless Terrorist Surveillance Program to the FISA Amendments Act of 2008, Congress, and the executive branch eased restrictions on intelligence gathering to permit widespread information collecting and sharing.[83] Faced with the external threats from terrorist organizations, the executive, legislative, and judicial branches found a common purpose in approving greater communication between the intelligence and law enforcement communities.[84] However, the government made many of these expansions in secret or without significant public discussion.[85] As these programs became public, the public raised concerns about the expansive and intrusive intelligence tools given to law enforcement. The concerns raised about these new intelligence-gathering authorities mirrored those raised forty years before.

B. Rising Concerns of Misuse of the New FISA Programs

Although changes to FISA noted in Section A were debated and enacted in public, other intelligence gathering programs were created in secret.[86] These programs came to be through executive actions and expansive, but classified, interpretations of FISA by the

---

[81] 50 U.S.C. § 1804(a)(6)(B) (2006).
[82] 122 Stat. at 2473.
[83] *See* Jewel v. NSA, No. 08-cv-04373, ¶ 6 (N.D. Cal. Dec. 20, 2013). In 2007, Congress passed the Protect America Act, which expired in February 2008. Pub. L. No. 110-55, 121 Stat. 552 (2007); 122 Stat. at 2473.
[84] *See Jewel*, No. 08-cv-04373, at ¶ 6.
[85] *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005) (discussing the leak of the secret Terrorist Surveillance Program), http://www.nytimes.com/2005/12/16/ politics/bush-lets-us-spy-on-callers-without-courts.html?_r=0; Glenn Greenwald et al., *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, THE GUARDIAN (Jun. 11, 2013) (which exposed the leaked information on the bulk collection of metadata and other classified programs) http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.
[86] Risen & Lichtblau, *supra* note 85; Greenwald et al., *supra* note 85.

FISC.[87] The world learned of these secret intelligence tools through leaks of classified information and authorized declassification by the executive branch.[88] The reaction to these intelligence tools caused a significant debate and calls for restrictions on intelligence gathering.[89]

On October 4, 2001, President George W. Bush secretly authorized the Terrorist Surveillance Program, permitting the National Security Agency ("NSA") to wiretap communications from members of Al Qaeda to individuals within the United States.[90] The President later claimed that he had executive authority, based in the Constitution itself, to conduct this action.[91] These wiretaps were conducted outside of the FISA process and without any judicial oversight or approval.[92]

Eventually, a leak and subsequent confirmation by the Executive made the Terrorist Surveillance Program public.[93] Many experts argued these wiretaps were illegal under FISA or another federal law.[94] One federal district court agreed, determining that the program violated the Constitution because it permitted searches without judicially authorized warrants.[95] Instead of appealing the decision, the executive branch sought Congressional approval for the program.

---

[87] *See* Public Declaration of James R. Clapper, Director of National Intelligence at 6, Jewel v. NSA, No. 07-cv-693-JSW (N.D. Cal. Dec. 20, 2013); *see In re* Application of the FBI for the Production of Tangible Things (2013) (No. BR 13-80, http://www.dni gov/files/documents/PrimaryOrder_ Collection_215.pdf [hereinafter *In re* Application of the FBI].

[88] Risen & Lichtblau, *supra* note 85; Greenwald et al., *supra* note 85.

[89] Serwer, Adam, *New calls for surveillance reform after Snowden,* MSNBC (September 25, 2013), http://www.msnbc.com/msnbc/new-calls-surveillancereform-after.

[90] Risen & Lichtblau, *supra* note 85; *see* Public Declaration of James R. Clapper, Director of National Intelligence, *supra* note 87, at 6.

[91] U. S. DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT 5, 17 (2006), http://www. usdoj.gov/opa/whitepaperonnsalegal authorities.pdf.

[92] *Id.*

[93] Risen & Lichtblau, *supra* note 85.

[94] *Id.*

[95] ACLU v. NSA, 438 F. Supp. 2d 754, 775-82 (E.D. Mich. 2006).

C. *Responses to the Post-9/11 Expansion of Federal Investigatory Authority*

Congress eventually agreed to a modified version of the program and passed the FISA Amendment Act of 2008.[96] The legislative solution in response to the Terrorist Surveillance Program's warrantless wiretaps had its own potential drawbacks because it legislated an avenue for the government to obtain wiretaps *without* a judicially authorized search warrant.[97]

Section 702 of FISA Amendment Act permitted the executive branch to conduct warrantless wiretaps of foreign persons outside the United States to gather foreign intelligence.[98] The FISC has limited involvement; it merely approves the targeting and minimization procedures used generally by the intelligence community, but it does not approve individual surveillance.[99] In addition, the FISC does not approve any individual interception, nor does it determine that there is probable cause the interception will gather foreign intelligence information.[100]

Since the inception of Section 702 interceptions, there have been numerous mistakes, misuses, and abuses of the program.[101] Individual intelligence analysts have made improper queries without permission, have queried Section 702 databases accidentally, and have queried Section 702 databases for U.S. persons when they should have only queried foreign nationals.[102] There have also been

---

[96] In 2007, Congress passed the Protect America Act, which expired in February 2008. Pub. L. No. 110-55, 121 Stat. 552 (2007). The FISA Amendment Act was passed in 2008 and is still current law; Pub. L. No. 110-261, 122 Stat. 2463, 2473 (2008).

[97] 122 Stat. at 2473.

[98] Procedures for Targeting Certain Persons Outside the United States Other than United States Persons, 50 U.S.C. § 1881a(a) (2015).

[99] 50 U.S.C. § 1881a(a).

[100] *Id.*

[101] 158 CONG. REC. S8457 (daily ed. Dec. 28, 2012) (Statement of Sen. Feinstein).

[102] *See* U.S. DEP'T OF JUSTICE, SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUES PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, 33 (2013), http://www. dni.gov/files/documents/ Semiannual%20 Assessment%20of%20Compliance%20with%20procedures%20 and% 20guide lines%20issued%20pursuant%20to%20Sect%20702%20of%2FISA.pdf.

systematic errors, where the collection system collects too much information because of technical errors without solutions.[103] In short, the government conceded that its collection process is flawed and a certain portion of its interceptions will be wholly domestic communications.[104] The government admitted that it could not conduct the program without a small portion of its activity being outside of its permissible interception. So far, no court has ruled that the Section 702 program is per se unlawful because of this problem, but this issue is just beginning to be reviewed in federal courts.

The Terrorist Surveillance Program and the enactment of Section 702 were not the only programs that permitted the warrantless collection of information. The disclosure of classified surveillance programs by Edward Snowden created significant public outcry.[105] Although the programs disclosed by Snowden dealt with the interception of "metadata" and not the content of communications, the collection of vast amounts of information on ordinary Americans caused a national uproar.[106] This program—approved by the FISC based on an expansive reading of a section of FISA relating to the search of business records—permitted the government to collect limited information on all Americans (a bulk collection), on the condition that it could not be searched unless the government had specific suspicion that it was connected to foreign intelligence.[107]

The program leaked by Snowden was approved by the FISC but it nonetheless raised concerns similar to those found during the

---

[103] *Id.* at 32.
[104] 50 U.S.C. § 1881a(a).
[105] Greenwald et al., *supra* note 85.
[106] *Id.*; *see also In re* Application of the FBI, *supra* note 87.
[107] *See* 50 U.S.C. § 1861 (2015) (commonly referred to as Section 215). *See* Office of the Dir. of Nat'l Intelligence Pub. Affairs Office, Newly Declassified Documents Regarding the Now-Discontinued NSA Bulk Electronic Communications Metadata Pursuant to Section 402 of the Foreign Intelligence Surveillance Act (Aug. 11, 2014), http://www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/1099-newly-declassified-documents-regarding-the-now-discontinued-nsa-bulk-electronic-communications-metadata-pursuant-to-section-401-of-the-foreign-intelligence-surveillance-act?highlight= WyJuZXdseSIsImRlY2xhc3 NpZmllZCIsIm5ld2x5IGRlY2xhc3NpZmllZCJd.

Church Committee 45 years earlier.[108] The public concern was that current oversight of the government's use of intelligence tools was insufficient to protect the liberties of everyday Americans.[109] Public perception once again shifted to the belief that the government was misusing these intelligence tools to spy domestically on Americans with little connection to national security.[110] The courts eventually weighed in, and the Second Circuit Court of Appeals ruled that this bulk collection program is inconsistent with the statutory language of FISA, and thus, is unlawful.[111] Any information gathered from the bulk collection program is now likely inadmissible in a criminal prosecution as the fruit of an illegal search.[112]

Congress responded to these concerns and eliminated the government's bulk collection of limited information on Americans, but it transferred this collection to private companies who are required to retain information they collect and have it available for search.[113] Only time will tell if this revision meets with the Court's interpretation of the statute and the Fourth Amendment to the Constitution, and if Congress and the Executive will remain satisfied that this revised provision achieves the appropriate balance between civil liberty and national security.

---

[108] CHURCH ET AL., *supra* note 44, at 5-6; Diane C. Piette & Jesselyn Radack, *Piercing the "Historical Mists:" The People and Events Behind the Passage of FISA and the Creation of the "Wall*," 17 STAN. L. & POL'Y REV. 437, 448 (2006).

[109]Greenwald et al., *supra* note 85.

[110] James Ball & Spencer Ackerman, *NSA Loophole Allows Warrantless Search for US Citizens' Emails and Phone Calls*, THE GUARDIAN (Aug. 9, 2013), http://www.the guardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls; Laura K. Donohue, *NSA Surveillance May be Legal—but it's Unconstitutional*, THE WASH. POST (June 21, 2013), http://www.washingtonpost.com/opinions/nsa-surveillance-may-be-legal--but-its-unconstitutional/2013/06/21/b9ddec20-d44d-11e2-a73e-826d299ff459_story.html.

[111] *Clapper*, 785 F.3d at 818-20.

[112] *See* 50 U.S.C. 1806(e) (2015) (providing that a defendant may move to suppress information that is unlawfully acquired).

[113] *See* Erin Kelly, *Senate Approves USA Freedom Act*, USA TODAY (June 2, 2015), http://www.usatoday.com/ story/news/politics/2015/06/02/patriot-act-usa-freedom-act-senate-vote/28345747/.

IV. PLANNING FOR CHANGE: WHAT INTELLIGENCE PROGRAMS ARE AT RISK TODAY

The debate over the Snowden-leaked program of bulk collection of information on Americans highlights the concern that national security professionals must face: how do they turn intelligence information into criminal evidence when they cannot be certain that current intelligence programs will be lawful at the time of trial? The program leaked by Edward Snowden was a statutory based collection program—FISA Section 215—reauthorized multiple times by the FISA Court before it was ultimately ruled unlawful.[114] If national security professionals cannot rely on judicial interpretations of statutory law to build cases, how can they continue to use the federal courts as a reliable solution to respond to current and future national security threats?

The answer involves risk analysis, something that is at the heart of intelligence analysis. When the legal climate is rapidly changing in the national security community, professionals must conduct a risk analysis of not only the threats to the nation, but also the risks that intelligence programs will become unavailable in the future, and render their evidence potentially inadmissible. A careful review of the past and present controversies around intelligence collection demonstrate three factors that national security professionals can use to evaluate the risk of losing intelligence tools and the information gathered from them. These factors are: (1) whether knowledge of the program is public or secret, (2) whether courts have approved the use of the program, and (3) whether the intelligence collection procedures resemble criminal evidence gathering procedures that courts are comfortable with allowing.

Turning to the first factor, classified sources and methods will eventually be made public—through leaks, declassification, or other means.[115] National security professionals must accept this as

---

[114] *See* In re Application of the FBI for an Order Requiring the Prod. of Tangible Things From [Redacted] (No. BR 15–24), at *3 (FISA Ct. Rev. Feb. 26, 2015); *see also Clapper*, 785 F.3d at 801-02, 820-22, 826 (finding the program was unlawful).

[115] *See, e.g.*, Risen & Lichtblau, *supra* note 85; Greenwald et al., *supra* note 85; David Kravets, *Declassified Documents Prove NSA is Tapping the Internet*, WIRED

fact. Each time one of the classified intelligence programs mentioned above was made public, there were negative consequences for both the intelligence program and the information gained from it.[116] The Terrorist Surveillance Program was leaked to the media and later confirmed by the President.[117] Subsequently, a district judge found the program to be unlawful.[118] Edward Snowden leaked the Section 215 bulk data collection program—and a federal appellate court found that the program was unlawful.[119] There is a lesson to be learned from this: intelligence gathering programs that the government keeps secret carry increased risk that they will be determined to be unlawful when the public finally learns about them.

The general public can learn about many intelligence programs through publicly available information like the statutes that authorize their use. The programs are public knowledge even though their use in a particular case is classified.[120] Traditional FISA warrants are a perfect example.[121] While the targets of FISA warrants are classified, the program itself is not. Both Congress and the courts recognize the program, the process to obtain warrants, and their use. These public intelligence programs carry less risk that they will be unavailable in the future.

MAGAZINE, Aug. 21, 2013, http://www.wired.com/2013/ 08/nsa-tapping-internet/ (declassified); John Diamond & David Jackson, *Surveillance Program Protects Country, Bush Says,* USA TODAY (Jan. 23, 2006), http://usatoday30.usatoday.com/ news/washington/2006-01-23-bush_x.htm (other means, like spontaneous Presidential confirmation).

[116] *See, e.g.*, Donohue, *supra* note 110; Risen & Lichtblau, *supra* note 85; Greenwald et al., *supra* note 85; *See* Julian Hattem, *Time for a New Church Committee? Ex-Staffers Think So*, THE HILL, Jan. 27, 2015, http://thehill.com/policy/technology/ 230822-time-for-a-new-church-committee-ex-staffers-think-so; Ball & Ackerman, *supra* note 102.

[117] Risen & Lichtblau, *supra* note 85; Greenwald et al., *supra* note 85; Diamond & Jackson, *supra* note 115.

[118] ACLU v. NSA, 438 F. Supp. 2d 754, 782 (E.D. Mich. 2006).

[119] *Clapper*, 785 F.3d at 793.

[120] *See generally*, 50 U.S.C. §§ 1801-1805 (2015) (traditional FISA warrants for wiretaps); 50 U.S.C. § 1861 (2015) (permits collection of business records without bulk collection).

[121] 50 U.S.C. §§ 1801-1805.

The second factor pertains to the legal risk for classified programs. Intelligence programs that require court approval are more likely to endure than those done without judicial oversight. The more input a judicial officer had in approving the collection of information, the more likely a subsequent judge will permit the introduction of that information as evidence in court. The gathering of information under Executive Order 12333 and FISA Section 702 are examples of programs that have less judicial oversight.[122] This lack of judicial input during collection creates risk that a court overseeing the admission of that evidence in a criminal case will determine it is inadmissible. Programs that involve judicial officers in the process and obtain judicially sanctioned collection efforts are far more likely to be sustained in the future. The Section 215 bulk collection program may seem like an exception, but it actually proves the point.[123] The court ruled that the program violated the statute.[124] The bulk collection program is an example of an intelligence program that has risk of being lost because it was conducted in secret and without any corollary to a traditional criminal program.[125]

Third, the risk of having programs overturned is lower when using intelligence programs that have similarities to ordinary criminal investigative tools. When attempting to turn intelligence information into criminal evidence it helps to work with an intelligence program that has similar procedures to traditional criminal tools. Again, traditional FISA wiretaps are a good example. FISA wiretaps require an application to a judge, with a sworn affidavit, where a judge finds probable cause, and issues a limited warrant.[126] While the specific procedures and findings differ from a criminal Title III warrant, the similarities between the intelligence tool and the criminal tool make it more palpable to courts and juries to accept the evidence.[127] Using tools that have no corollary in the criminal system raises concerns that the information was obtained without following the normal checks on government conduct.

---

[122] *See* Exec. Order No. 12333, 46 F.R. 59941 (1981); 50 U.S.C. § 1802.
[123] 50 U.S.C. § 1861 (permits an order to produce certain business records).
[124] *See Clapper*, 785 F.3d at 826.
[125] *Id.*; 50 U.S.C. § 1861.
[126] *See* 50 U.S.C. § 1805.
[127] *Compare* 50 U.S.C. §§ 1801-1804 *with* Fed. R. Crim. P. 41.

Courts are more likely to question the tool's legality if it was not involved in the process to use the tool.

V. CONCLUSION

Our nation has only begun to evaluate what changes to make to the current intelligence programs. United States history demonstrates that Congress, the courts, and the executive branch will constantly struggle with the balance of giving national security professionals the tools needed to protect the nation from threats and giving our citizens the protections needed to secure their civil liberties. Intelligence professionals need to carefully examine the current use of intelligence programs because these programs, and how they can be used, will change. Some intelligence programs will be modified and restricted. Others will be removed by executive, legislative, or judicial action.

National security professionals who must transform intelligence into evidence in criminal cases must be especially wary. Courts may review intelligence programs in the future and retroactively determine they were unlawful. Any evidence law enforcement gathers pursuant to those programs may not be admissible when the national security case gets to trial. But a cautious national security professional can carefully decide which of the currently available intelligence collection options are likely to both meet the current collection requirement and also endure increased scrutiny so the information is useful in the future. Intelligence professionals excel at risk analysis; now they must use those skills to evaluate the durability of the collection programs available to them. FISA will change again, and national security professionals must be prepared for these changes.

QUANTUM LAWMAKING: HOW NATIONAL SECURITY LAW HAPPENS WHEN WE'RE NOT LOOKING

Jesse Medlong*

Lower-order laws are increasingly unstable and uncertain the further their authority descends from the Constitution. That is because those laws become susceptible to successively greater constraints from higher-order laws. That uncertainty and instability do not, however, prevent such laws from leaving a mark on the world around them. In many regards, these laws superficially resemble some of the oddities of quantum mechanics, which governs the increasingly odd behavior of particles at the smallest levels. This article contemplates the theoretical and practical implications of the law's metaphorical similarities to quantum mechanics, particularly in the area of national security and military law. Quantum strangeness plays a more salient role in that body of law for several reasons, including the unique legal role of delegated authority and standard operating procedures in the military, how courts resolve legal challenges to military orders, the unusually strong organizational-behavior effect that military orders have on national security policy, and the odd fact that military law is potentially more responsive to "the enemy" than to democratic stakeholders on the home front.

* International lawyer and litigation associate, DLA Piper LLP (US), and veteran of the United States Navy. MS in International Relations, Troy University; JD, University of Michigan. The author thanks Professor Julian Mortenson, whose advice and encouragement were essential to this article's publication. The views expressed in this article are the author's own, and they do not represent the views of his employers, past and present.

INTRODUCTION

At a glance, nothing seems terribly strange about national security law—and, in particular, military law. Specifically, the military is among the most longstanding policy instruments by which national governments pursue their interests. Indeed, the military's rigid hierarchy, highly structured bureaucracy, and elevation of culture and tradition might lend the impression that the military and its law are perfectly straightforward and not the sort of place in which abstract legal theories might thrive. That impression would be wrong. Despite a highly ordered legal structure starting with (in the United States) the Constitution and federal statutes, much of what goes on in the context of military law is strange and poorly understood, even by those immersed in it. This article seeks to explore the disparity between that impression and reality.

Beginning with military law's most commonplace attributes, the Uniform Code of Military Justice ("UCMJ") is the statutory framework governing the armed forces of the United States of America. Empowered by this and other statutes and by authority inhering in executive authority, Department of Defense ("DOD") officials and high-ranking military officers promulgate and implement regulations that bind over two million active duty and

reserve military members.[1] Thus far, this closely resembles the mundane and nearly ubiquitous interaction between congressional legislation and the delegation of "quasi-legislative" (and "quasi-judicial") power to executive agencies. But there is an important difference. For administrative lawmaking, the analysis essentially ends there.[2] In the military context, however, this bifurcation between legislation and regulation is merely the beginning.

The UCMJ provides a conduit for further delegation through three of its punitive articles: Article 90 (Assaulting or willfully disobeying a superior commissioned officer); [3] Article 91 (Insubordinate conduct toward a warrant officer, noncommissioned officer, or petty officer);[4] and Article 93 (Failure to obey an order or regulation).[5] These articles endow any lawful order—which can be spoken or written, of either general or particular applicability, and

[1] *See* OFFICE OF THE UNDER SEC'Y OF DEF., PERS. AND READINESS, POPULATION REPRESENTATION IN THE MILITARY SERVICES, FISCAL YEAR 2009 REPORT 2 (2009).
[2] *See* Synar v. United States, 626 F. Supp. 1374, 1398 (D.D.C. 1986) (acknowledging that "'quasi-legislative' and 'quasi-judicial' functions can no longer be regarded as extraordinary or even unusual activities of executive agencies.").
[3] Assaulting or Willfully Disobeying Superior Commissioned Officer, 10 U.S.C. § 890 (1956) ("Any person subject to this chapter who-- (1) strikes his superior commissioned officer or draws or lifts up any weapon or offers any violence against him while he is in the execution of his office; or (2) *willfully disobeys a lawful command of his superior commissioned officer*; shall be punished, if the offense is committed in time of war, by death or such other punishment as a court-martial may direct, and if the offense is committed at any other time, by such punishment, other than death, as a court-martial may direct.") (emphasis added).
[4] Insubordinate Conduct Toward Warrant Officer, Noncommissioned Officer, or Petty Officer, 10 U.S.C. § 891 (1956) ("[a]ny warrant officer or enlisted member who-- (1) strikes or assaults a warrant officer, noncommissioned officer, or petty officer, while that officer is in the execution of his office; (2) *willfully disobeys the lawful order of a warrant officer, noncommissioned officer, or petty officer*; or (3) treats with contempt or is disrespectful in language or deportment toward a warrant officer, noncommissioned officer, or petty officer, while that officer is in the execution of his office; shall be punished as a court-martial may direct") (emphasis added).
[5] Failure to Obey Order or Regulation, 10 U.S.C. § 892 (1956) ("[a]ny person subject to this chapter who-- (1) *violates or fails to obey any lawful general order or regulation*; (2) having knowledge of any other lawful order issued by a member of the armed forces, which it is his duty to obey, *fails to obey the order*; or (3) is derelict in the performance of his duties; shall be punished as a court-martial may direct") (emphasis added).

"standing"[6] or *ad hoc*—with the force of law. An affected military service member's failure to follow any such order can result in criminal liability. The orders themselves (much like statutes and agency actions) can be subject to judicial review if they are challenged as unlawful. Thus, a wide range of lawful orders—including actions as varied as intraoffice policies, standard operating procedures ("SOPs"), and battlefield orders—possess many of the characteristics one would commonly ascribe to law. But the authority to issue lawful military orders is no ordinary delegation.

There are profound differences between the processes that produce these orders and the traditional exercise of delegated legislative authority. Rules enunciated in lawful orders are highly dynamic: they can be changed instantly and without prior notice, and they often cease to exist once they are carried out.[7] In these ways, lawful orders (and especially what this article refers to as "battlefield orders") resemble orders delivered in agency adjudications.[8] But lawful military orders—and especially standing and general orders—also closely resemble administrative rules. They have future effect and are, in the words of the Administrative Procedures Act ("APA"), "designed to implement, interpret, or prescribe law or policy or describ[e] the organization, procedure, or practice requirements of" a military organization or unit, or even the conduct of an individual service member.[9] Moreover, whereas legislation and regulation

[6] A standing order is "one of a number of orders which have or are likely to have long-term validity." *Standing Order*, COLLINS ENGLISH DICTIONARY, http://www.collinsdictionary.com/dictionary/english/standing-order (last visited Nov. 29, 2015).
[7] We might therefore think of lawful orders (other than general orders) as containing built-in sunset provisions. *See Sunset Provision*, COLLINS ENGLISH DICTIONARY, http://www.collinsdictionary.com/dictionary/english/sunset-clause (last visited Dec. 1, 2015) (defining "sunset provision" as "a provision of a law that it will automatically be terminated after a fixed period unless it is extended by law.").
[8] *See* Administrative Procedures Act [APA] § 6, 5 U.S.C. § 551 (2011) (defining an order as "the whole or a part of a final disposition . . . of an agency in a matter other than rule making").
[9] *Id.* An interesting debate is currently ongoing in the world of administrative law over whether the APA aptly differentiates rules from orders. The APA differentiates these two kinds of actions according to their effect in time. Specifically, rules have *future* effect, whereas an adjudication is supposedly confined in the amber of the present, its posture affected only by those things that precede it. Thus, because an order is defined in the negative ("final disposition . . . *in a matter other than rule*

should ideally be responsive to the country's citizenry, many military orders are primarily responsive to "the enemy," whose aims presumably run counter to the desires of the public at large.[10]

The kind of law embodied by lawful orders—if it is law at all—departs so radically from our expectations of legally binding rules, that one must either reject its designation as *law* altogether or employ a different conceptual vocabulary to effectively describe it. This article posits that lawful military orders are undeniably law and proposes a framework from which to derive the requisite vocabulary. Specifically, its thesis suggests a continuum of lawmaking activity. At one end of the continuum lies what one might describe as "classical lawmaking." At the other extreme is "quantum lawmaking," in which the oddities described above tend to congregate. In describing this latter extremity, this article uses the language of quantum mechanics. The purpose of this Article is to provide substance for this metaphorical continuum, to apply this conceptual framework to the law of military orders, and to explain why the legal force of military orders matters outside the military itself.

Part I introduces the concept referred to in this article as quantum lawmaking. It explains how this metaphor can deepen our understanding of the law of military orders, as well as where along the proposed continuum this and other kinds of law fit. Part II discusses the legal issues implicated by the quirks of quantum lawmaking in the military setting. Part III describes some of the policy implications of having a body of law that not only maps onto

---

making"), the entire distinction seems to be that rules are prospective in effect and that orders are not rules. *See id.* The debate focuses on whether it would be more appropriate to differentiate these two kinds of action based on their applicability. If these would-be reformers have their way, rules would be redefined as agency actions of general applicability, and orders would become agency actions of particular applicability. *See* A.B.A. HOUSE OF DELEGATES, DAILY JOURNAL: 2005 MIDYEAR MEETING 2, 7 (2005), http://www.americanbar.org/content/dam/aba/migrated/leadership/2005/midyear/daily/hod_2005_midyear_meeting_daily_journal.doc. This kind of reform would to some extent lighten the ontological chore of classifying military orders according to the APA's definitions.

[10] *See, e.g.*, *Learn the 11 Military General Orders*, MILITARY.COM, http://www.military.com/join-armed-forces/military-general-orders.html (last visited Dec. 21, 2015) (outlining the 11 General Orders common to all of the U.S. Armed Forces).

the extreme end of the quantum lawmaking continuum but also profoundly affects our national foreign policy. But first, what *is* quantum lawmaking?

I. "QUANTUM LAWMAKING" AND THE SPECIAL CASE OF THE MILITARY

"[T]hose who are not shocked when they first come across quantum theory cannot possibly have understood it." ~ Niels Bohr[11]

Because I endeavor to co-opt the language of quantum physics to illustrate my thesis, a basic survey of that language is due. But before I delve into the quantum lexicon, I must first supply an important caveat: the metaphor has limits. I do not suggest that some platonic "Quantum Form" underlies both the smallest scale of the physical world and some odd species of lawmaking. Rather, I suggest that within the discipline of quantum mechanics resides a vocabulary that, when applied by way of metaphor to certain kinds of law, helps to illuminate otherwise-obscure aspects of that law. This metaphor should not be laid alongside the law of military orders—or, indeed, any kind of law—and compared point by point. Doubtless, such examination would unveil ample disjuncture between the metaphor and reality. But insofar as this borrowed vocabulary helps to fill a hole in our current understanding of the law of military orders, the rhetorical risk seems worth the gain.[12]

[11] WERNER HEISENBERG, PHYSICS AND BEYOND 206 (Ruth Nanda Anshen ed., Arnold J. Pomerans trans., 1971) (quoting Niels Bohr).

[12] Even with this caveat in place, I owe an apology to anyone who would rightly object to such a cursory depiction of those few principles of quantum theory necessary to my metaphor. The theory (including the concepts I briefly explore here) is immensely bizarre and intricate, is wildly successful at predicting experimental outcomes, and is done a disservice by this shortest of shrifts. *See, e.g.*, LISA RANDALL, WARPED PASSAGES: UNRAVELING THE MYSTERIES OF THE UNIVERSE'S HIDDEN DIMENSIONS 119-26 (2005). Sadly, the rest of the theory is well beyond the scope of this article and, I suspect, my own ability adequately to convey.

A. *Quantum Mechanics and the Strange World of the Infinitesimal*

Quantum mechanics is the field of physics concerned with the fundamental building blocks of existence.[13] Until the dawn of the "quantum revolution," scientific models explaining the universe and the forces animating it had been growing increasingly elegant and geometrically coherent. Culminating in Albert Einstein's theory of relativity, "classical physics" had revealed the universe to be a highly ordered place. Classical physics remains to this day the heart of our understanding of the universe's vastest features, from the graceful dance of galaxies to the structure of space-time itself. Classical physics begins to break down, however, when applied to the smallest phenomena. On this Lilliputian scale, one must rely instead on quantum physics.

While classical physics elegantly and continuously connects the outer expanses of the cosmos even to our own daily existence, quantum physics describes the omnipresent infinitesimal as a seething mathematical chaos, defying our basic assumptions not only about how the universe *is*, but also about how it *ought to be*. For a serious science, quantum physics can seem decidedly metaphysical.

Quantum mechanics is a discipline built unabashedly on uncertainty. One of the fundamental rules underlying quantum theory is the *uncertainty principle*,[14] which states that the universe's tiniest constituents invariably elude efforts to measure both their positions and motions at any given time.[15] Although early formulations of this principle suggested that the uncertainty was due to the limitations imposed by the technology available for making

---

[13] OXFORD UNIV. PRESS, OXFORD DICTIONARY OF PHYSICS 414-15 (John Daintith ed., 5th ed. 2005) ("[a] system of mechanics based on []quantum theory, which arose out of the failure of classical mechanics and electromagnetic theory to provide a consistent explanation of both []electromagnetic waves and atomic structure.").

[14] Also known as "Heisenberg's uncertainty principle" and the "indeterminacy principle." *See id.* at 553.

[15] BRIAN GREENE, THE ELEGANT UNIVERSE 114 (1999).

such measurements, subsequent experiments reveal the principle to be a fundamental feature of the vanishingly small.[16]

Stranger still, subatomic particles cannot truly be said to *have* either position or motion until an observation is made of one or the other.[17] In an oft-cited experiment to determine whether light consists of particles or waves, researchers placed an opaque surface, with two slits cut into it, between a light source and a photographic plate. When the light source flooded the slits with light, the photographic plate revealed a pattern of parallel lines resulting from the waves of light interfering with one another as they flowed simultaneously through the apertures. This is analogous to two pebbles being dropped simultaneously into water such that the ripples radiating from each pebble's point of impact interfere with those of the other pebble. These interference patterns suggested that light travels in waves. But when the experimenters fired individual photons (which are fundamental units of light) sequentially at the slits, the interference patterns remained. It was as though each photon interfered with itself, going through *both slits at once*. The apparently fractured photon does not collapse into a "single" particle again until it reaches the photographic plate—unless a photon detector is placed so as to observe which slit the photons "select." Experiments revealed that a detector placed in this manner somehow forced a photon to choose one slit or the other. The photons would then behave properly from the slit to the photographic plate and arrive at their destination without interference.[18]

---

[16] *Id.*

[17] The passive voice here is no accident. An observation need not be made by any person or device in particular. Rather, virtually *any* imprint left on the universe by a quantum occurrence can serve as an observation. *See generally* Henry Krips, *Measurement in Quantum Theory*, THE STAN. ENCYCLOPEDIA OF PHIL. (Edward N. Zalta ed., 2013), http://plato.stanford.edu/archives/fall2013/ entries/qt measurement/. For instance, a single photon—the fundamental particle from which the electromagnetic force is composed—can be "observed," among other methods, by a photographic plate, a photon detector, or a measurement of another particle that interacts with the photon.

[18] *See* GREENE, *supra* note 15, at 110. Bizarrely, the detector need only be placed at one slit or the other. When one detector is so placed, the observation that the photon

As though solipsistic subatomic particles were not strange enough, quantum mechanics also describes a mechanism by which the universe can cheat the law of conservation of mass and energy.[19] That is the principle that matter and energy can neither be created nor destroyed, but only converted from one state to another. Hence, mass and energy are conserved. But while no "new" matter or energy can be created, particles can sometimes erupt suddenly into existence by borrowing energy from the universe, as long as they return the energy shortly thereafter.[20] These so-called *virtual particles* bubble up from the chaotic foam of the universe's hidden but highly energetic subatomic depths.

With particles popping in and out of existence and not being able to decide where they are unless they are being watched, it is understandable that Einstein, the elder statesman of classical physics (and remorseful pioneer of quantum physics),[21] could not accept quantum mechanics' bizarreness. Whereas Einstein saw the elegant geometry residing in the grand forces of the universe's design as "fine marble," he likened the material stuff within the universe—and, importantly, the particles that constitute that material stuff—with "low grade wood."[22] While he had long hoped to unify both classical and quantum physics by finding that the "wood" (that is, matter) is

did not pass through the detector's slit is sufficient to collapse the particle and negate the interference effect. *See id.*

[19] This law provides that the amount of mass (or energy) in a closed system will remain constant over time, though mass can change form (i.e., mass can convert to energy or vice versa). In other words, neither mass nor energy can be created or destroyed, though either can change to the other. Conservation of mass and energy is a bedrock principle of classical physics. *See* OXFORD UNIV. PRESS, *supra* note 13, at 92 ("[a] law stating that the total magnitude of a certain physical property of a system, such as its mass, energy, or charge, remains unchanged even though there may be exchanges of that property between components of that system. . . . [C]onservation of mass is a law of wide and general applicability, which is true for the universe as a whole, provided the universe can be considered a closed system (nothing escaping from it, nothing being added to it). . .. [I]f mass is conserved, the conservation of energy must be of equally wide application.").

[20] GREENE, *supra* note 15, at 115-16.

[21] *See* WALTER ISAACSON, EINSTEIN: HIS LIFE AND UNIVERSE 6-7 (2007).

[22] ALBERT EINSTEIN, OUT OF MY LATER YEARS 83 (1950).

also marble deep down, quantum mechanics attempts to consign the entire universe—marble and all—to wood.[23]

B. Quantum Mechanics and the Law

But what do these odd laws of physics have to do with laws of the man-made variety? At the risk of seeming banal, I will begin to answer that question by citing a dictionary. The first definition of *law* in Black's Law Dictionary is, "[t]he regime that orders human activities and relations through systematic application of the force of politically organized society, or through social pressure, backed by force, in such a society."[24] This is a broad definition (and only one of many even within Black's), but it is instructive in that it forces us to pin down some of the defining characteristics of *law* as examined here. The three most salient features of this definition of law are that it is (1) systematic, (2) societal, and (3) backed by force.[25] Thus, the meaning of law needed here is the sort that Judge Richard Posner terms "law as a source of rights, duties, and powers."[26] The question, then, is how these rights, duties, and powers look in practice.

Definitions aside, we think we have a good idea what law is. As Justice Potter Stewart might have put it, we probably assume we know it when we see it.[27] At the very least, we feel some confidence as to what the law is *not*.

---

[23] MICHIO KAKU, HYPERSPACE 112 (1994).
[24] *Law*, BLACK'S LAW DICTIONARY (10th ed. 2014).
[25] *Id.*
[26] RICHARD A. POSNER, THE PROBLEMS OF JURISPRUDENCE 220-21 (1990). Other concepts denoted by the word "law," according to Judge Posner, are "law as a distinctive social institution[—]that is the sense invoked when we ask whether primitive law is really law[—and] law as a collection of sets of propositions—the sets we refer to as antitrust law, the law of torts, the Statute of Frauds, and so on." *Id.* at 220-21.
[27] This, of course, is a reference to *Jacobellis v. Ohio*, in which a concurring Justice Potter Stewart famously wrote, concerning hardcore pornography: "[b]ut I know it when I see it . . .". Jacobellis v. Ohio, 378 U.S. 184, 197 (1964).

1. *Mead Corp.* and the Intuitive Appeal of Classical Law

This confidence was on proud display in *United States v. Mead Corp*.[28] At stake in *Mead Corp.* was the legal force of United States Customs Service classification "ruling letters." *Ruling letters* are decisions by point-of-entry customs field officers classifying imported goods according to tariff schedules. These ruling letters interpret the statutory customs scheme to determine the classification of incoming goods (day planners, in this case) as subject to or exempt from tariffs. Ordinarily, an executive agency's reasonable interpretation of its enabling statute is entitled to deference so long as it does not contradict Congress's express intent.[29] But these interpretations were different. In an eight-to-one decision, the Court dismissed the notion that these classification rulings—thousands of which issue each year from dozens of widely scattered field offices—could carry the force of law. But why?

Though the Court's conclusion rested primarily on the intricacies of congressional intent and administrative practice, Justice Souter voiced a visceral rejection of the notion that so many rulings issued in such a decentralized fashion could be *law*. "Any suggestion," he wrote, "that rulings intended to have the force of law are being churned out at a rate of 10,000 a year at an agency's 46 scattered offices is simply *self-refuting*."[30] In a lengthy dissent peppered with dire warnings, Justice Scalia railed against the Court's reasoning. But in a moment of grudging agreement, he noted of "[t]he Court's parting shot, that 'there would have to be something wrong with a standard that accorded the status of substantive law to every one of 10,000 "official" customs classifications rulings turned out each year from over 46 offices placed around the country at the Nation's entryways,' . . . *I do not disagree*."[31]

Surely this renunciation goes too far. The Social Security Administration disposes of over eight million claims for benefits

---

[28] *See* United States v. Mead Corp., 533 U.S. 218, 234 (2001).
[29] *Id.* at 226-27. This is known as the "*Chevron* doctrine." *See* Chevron, U.S.A., Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837, 842-43 (1984).
[30] *Mead Corp*., 533 U.S. at 233 (emphasis added).
[31] *Id*. at 258 n.6 (Scalia, J., dissenting) (quoting Souter, J.) (emphasis added).

every year, with most claims wending their way through a byzantine network of state and federal offices.[32] Yet no one seriously doubts that these dispositions, although subject to review, enjoy legal force. So something else must account for the incredulity expressed by both the majority and the dissent in *Mead Corp.* Very likely, there was something about the process or the "appearance" of this activity that Justices Souter and Scalia found incompatible with their preferred understanding of legally binding norms.[33] After all, society cannot just let some guy with a clipboard on a dock make *law*, can it?

Revealed in this curious dictum is a distaste for the idea that low-level employees in the peripheries of bureaucracy can make prescriptive, prospective, and generally applicable law. This suspicion is not of highly diffuse and prolific lawmaking authority, but rather of highly diffuse and prolific *rulemaking* authority. The fact is that society seems comfortable with Social Security claims being processed at rates vastly outstripping that at which customs rulings were being "churned out" (and at many more than 46 offices). This suggests that agency adjudications (to say nothing of judicial decisions generally) produce no similar suspicion that the fundamental substance of the law is being worked into a froth. When the law is already spelled out, we trust courts and even agency underlings to apply it, even when the effects of those decisions look

[32] *See* SOC. SEC. ADMIN., FISCAL YEAR 2012 BUDGET OVERVIEW 8 (2011). This figure includes "4.6 million retirement, survivor, and Medicare claims; approximately 3.3 million Social Security and SSI initial disability claims; and 349,000 SSI aged claims." *Id.* This claims figure does not speak at all to the number of appeals processed, which the SSA totals as "approximately 744,000 reconsiderations, 823,000 hearings, and 140,000 Appeals Council appeals." *Id.*

[33] An alternative explanation is that Justices Souter and Scalia, while still sweeping too broad in their protestations, did not mean that such rulings cannot have *any* force of law. Rather, we might conclude, they meant to suggest that classifications rulings issued in this manner cannot have *this kind* of legal force. This explanation allows for the possibility that other forms of legal force might proceed from various governmental actions (e.g., informal adjudications by the SSA), but that they must be more clearly adjudicatory in nature. By this formulation, even these very customs rulings might have legal force if they were purely adjudicatory in function and not implicitly creating binding and forward-looking norms. In either event, I feel confident that the "self-refuting" criteria to which the Court adverts cannot be taken literally.

an awful lot like new rules.[34] To allow low-level bureaucrats to *prescribe*, on the other hand, seems beyond the pale. This is not so unlike Einstein's visceral rejection of the principles of quantum mechanics. Just as these justices found it "self-evident" that law cannot be made in such a *vulgar* fashion, Einstein just "knew" on some basic level that the universe could not ultimately be cut from "low grade wood."[35] History has not been kind to Einstein's skepticism; the incredulous dictum from *Mead Corp.* deserves no greater favor.

This discomfort complements (and is likely the progeny of) the simplest narrative of the law: legislators craft laws and judges interpret and apply them. These laws are largely stable, which is to say they remain in force either until the legislature changes them through the same laborious process by which they were forged, or until a court invalidates them. This, then, is "classical" law. And aside from the observation that "laws, like sausages, cease to inspire respect in proportion as we know how they are made,"[36] most people—Supreme Court justices notwithstanding—probably find this a more tasteful sort of law than what might be promulgated by guys on docks with clipboards.

But this polished marble of formalism and stability loses its luster under closer scrutiny. As alluded to above, the stability of even statutory law is not absolute: courts can find a statute unconstitutional. When that happens the law disappears and is no more. Hovering about the tombs of such laws is the philosophical question of whether an unconstitutional law was ever a law at all. It is one thing to make a metaphysical pronouncement such as "an unconstitutional law is void, and is as no law"[37] or that it "is no law at

[34] As Justice Murphy explained in the landmark *Securities and Exchange Commission v. Chenery Corp.*, agencies can use the adjudicatory mechanism to "announc[e] and appl[y] a new standard of conduct" even when such announcement or application has retroactive effect. SEC v. Chenery Corp., 332 U.S. 194, 203 (1947). After all, he noted, "[e]very case of first impression has a retroactive effect." *Id.*

[35] *See* ISAACSON, *supra* note 21, at 336–37 (2007).

[36] *An Impeachment Trial*, U. CHRON., U. OF MICH., Mar. 27, 1869, at 4 (quoting poet John Godfrey Saxe).

[37] *Ex parte* Siebold, 100 U.S. 371, 376 (1879).

all."[38] It is quite another to pretend that these laws do not possess all the attributes and produce all the effects—including obedience and reliance—of other systematic and force-backed societal rules until that fateful day when they are pronounced "no law at all."

One need look no further than the Supreme Court's decision in *Stern v. Marshall* to see how a statute long adhered to can be unceremoniously rendered a non-law.[39] *Stern* held that a statutory provision concerning certain bankruptcy-related common-law counterclaims was unconstitutional.[40] So-called *Stern* claims are compulsory counterclaims arising in a bankruptcy that do not constitute core proceedings under the bankruptcy. Congress, pursuant to its bankruptcy power, had granted jurisdiction over such claims to the Article I bankruptcy courts. The Supreme Court held that this jurisdictional provision violated the grant of the judicial power in Article III, meaning that all prior final judgments on *Stern* claims had been, unbeknownst to the litigants, invalid.[41] Can one really say with a straight face that every bankruptcy judge, every party filing a state-law counterclaim, every party abiding by a ruling in such a counterclaim, was merely going through the motions of an elaborate pantomime that had literally *nothing* to do with the law? And if one insists this is the case, is such a formulation anything other than academic?

---

[38] Tyler v. Dane County, 289 F. 843, 846 (W.D. Wis. 1923). This is itself a reformulation of the Augustinian axiom that "an unjust law . . . is no law." SAINT AUGUSTINE THE TEACHER: THE FREE CHOICE OF THE WILL, GRACE AND FREE WILL 81 (Robert P. Russell, trans. 1968). American jurisprudence, however, pares back this broader statement as elevating "natural law" above the Constitution. *See, e.g.*, Calder v. Bull, 3 U.S. 386, 398-99 (1798) (opinion of Iredell, J.). Of course, for Saint Augustine natural law *was* fundamental in just the way that the Constitution is to the U.S. government, so it is reasonable to find a certain equivalence in the philosophical postulates these axioms share.

[39] *See* Stern v. Marshall, 131 S. Ct. 2594, 2620 (2011).

[40] Procedures. 28 U.S.C. § 157(b)(2)(C) (2005).

[41] Subsequent cases have softened *Stern*'s impact by clarifying its scope, but these decisions would not necessarily spare these pre-2011 *Stern* claims. *See* Exec. Benefits Ins. Agency v. Arkison *(In re Bellingham Ins. Agency, Inc.)*, 134 S. Ct. 2165, 2168 (2014); Wellness Int'l Network, Ltd. v. Sharif, 135 S. Ct. 1932, 1946-47 (2015).

2. Virtual Law As an Alternative to Non-Law

There is an alternative formulation. A law passed, codified, and obeyed but later invalidated can be seen as having been a law in every meaningful respect until the point at which it was struck down, at which point it merely vanishes. It is a "virtual law," akin to the "virtual particles" described above, its collapse precipitated by judicial observation. The practical effect is no different from that of a statute repealed through the legislative process. The legal force borrowed from the constitutional universe disappears back into the ether from which it sprang. Its past effects persist, but to all who later act within the virtual law's ambit, the law is mere memory.[42] Thus, the only truly "classical" law (i.e., law that cannot be struck down or changed by terms other than its own) is the Constitution. By definition, there can be no "unconstitutional" provision of the Constitution. Move one step away from that underlying fabric of the legal universe, and laws remain fairly classical by all appearances, but one cannot assume their stability without question. Statutes (as well as treaties passed in accordance with Article II of the Constitution),[43] then, occupy the first step on the spectrum away from classical law and toward what I call *quantum law*.

Key to this model is the role of what I have referred to as *judicial observation*. Judicial observation does not reveal only whether a law is "real" or "virtual." Judicial observation, like an observation in a physicist's laboratory, fixes some quality of its object relative to the world around it. By interpreting the law, judges shake the uncertainty from that law's practical manifestation. If judges are the observers and the laws are what judges observe, then higher-

[42] This formulation might well understate the impact of the ripples created by an invalidated law's past effects. Outcomes in legal disputes do not exist in a vacuum, so when an earlier disposition is premised on a law that is later overturned, the effects emanating from that disposition interact with other occurrences just as they would if the law had never been invalidated. An adverse disposition in a bankruptcy suit can spell the difference between poverty and plenty, and—whatever the Supreme Court says *ex post facto* of the process involved—each of these outcomes would itself produce economic and social effects that are not isolated to the litigants in the proceeding. Thus, even if we accept that "an unconstitutional law is no law at all," this cannot mean that it is *nothing* at all. *See Tyler*, 289 F. at 846.

[43] U.S. CONST. art. VI, cl. 2.

order laws provide constraints much like the slits in our experiment. The legislative process produces a law, the effects of which are felt by those the law governs, including entitlement recipients, regulators, regulated entities, and regulatory beneficiaries. But when a judicial observation is brought to bear on a particular law in a particular situation (the judicial equivalent of an experiment), the law either passes through the obstacle course of superior laws or it does not. And when that law is held to pass within the range (or ranges) permitted by the regimes to which it is subject, we also know whether the particular application under review is permissible. In other words, the court tells us whether the challenged law passes through the "slits" (that is, constraints imposed by higher-order law) and which slit it passes through.

Here is a quick illustration. Suppose Congress passes and the President signs a bill banning the use of subversive physics metaphors in law-review articles. Until someone instigates an "experiment" (that is, challenges the statute in court), the effects of the law multiply and interact with one another unimpeded. Even before the experiment, the Constitution is a theoretical slit to which the law must conform. Before launching the experiment, however, no one is manning the slit: maybe the law finds its way through, and maybe it does not. But once some oppressed author sues over this content-based restriction on expression, the court brings its sensors to bear on the question whether this law has in fact passed through the independent constraint. If the court's observation finds this law to be improperly calibrated, the law is overturned, and its failure to navigate the obstacles is confirmed. But just as a photon can have the effect of going through both slits at once despite its inability to perform the underlying feat when observed, the law can have the effects associated with having conformed to its own constraints even though it was invalidated as "no law at all." Put another way, the past effects of this law were real, and they do not go away, but the law has no further effect going forward.

So potent a force is judicial observation in our legal reality—and so pervasive is uncertainty—that even the paradigmatic classical law of the Constitution can be forced to conform to its strictures. To cite a famous example, one might ask what is meant by the term

"privileges or immunities of citizens of the United States."[44] The vast majority of Americans might understand the phrase one way, and many meanings—each conveying a slightly different nuance—are possible. But the Court's interpretative observation in the *Slaughter-House Cases* confirmed only one.[45]

Admittedly, at this level of analysis, a quantum model adds little to our understanding of judicial interpretation. But describing higher-order laws as mile markers at which a law can be observed and its inherent uncertainty collapsed sets the stage for the layers of law that lie far beneath the Constitution's "classical" veneer.

Beyond statutory law, administrative regulations are yet another step further down this spectrum. Regulatory laws vary from higher-order laws in several regards. First, courts can strike down a regulatory law for constitutional infirmity, as well as for violating its enabling statute or even some other statute. Second, the processes for creating legislative rules in the administrative context are less centralized and less formal than legislation. Third, regulations are more vulnerable to repeal than statutes: whereas only another statute can repeal a statute,[46] regulations are subject to repeal both by statutes and by the rulemaking process that created them.

Then there is state law. State constitutions are subject to all of the previously mentioned breeds of federal law, so they are theoretically even less stable. Nevertheless, there are large areas over which these separate authorities do not overlap. So, for instance, courts seldom confront federal regulation that preempts a state's constitution.[47] State statutory and regulatory laws are subject to still

[44] U.S. CONST. amend. XIV, § 1, cl. 2.

[45] Slaughter-House Cases, 83 U.S. 36, 74 (1872). Note that it would go too far to say that the Court invalidated all but one. In reality, the Court foreclosed many, if not most, readings of the Privileges or Immunities Clause, but some residual uncertainty inevitably remains. Because this clause is viewed essentially as a dead letter, that remaining modicum of uncertainty will likely persist into the foreseeable future, like a jurisprudential Schrodinger's cat, indefinitely suspended between living and not.

[46] That is, by bicameral passage and presentment to the President. U.S. CONST. art. I, § 7, cl. 2.

[47] The rarity of this situation is doubtless augmented by substantive canons of interpretation that erect presumptions against implicit preemption of state law. *See,*

more overriding legal constraints to which they must conform if they are to survive. Thus the image that emerges is of a linear relationship among different bodies of law and their distance from pure classical law (the Constitution).[48] That distance corresponds to relatively greater degrees of instability accompanied by relatively less pomp in their formation.[49] Nevertheless, the congeries of legislative activity described thus far still constitutes a mundane sort of law. Although a hint of quantum character begins to show through, nothing is particularly bizarre about the theoretical fraying that occurs when legislative authority is delegated or, as is the case in our federal system, divided between two distinct political spheres. But these

e.g., Rice v. Santa Fe Elevator Corp., 331 U.S. 218, 230 (1947) ("we start with the assumption that the historic police powers of the States were not to be superseded by the Federal Act unless that was the clear and manifest purpose of Congress."). Canons such as this—as well as those erecting presumptions against derogation of common law and derogation of customary international law absent express intent—have the effect of maximizing the instability of higher-order laws vis-à-vis lower-order laws in that they broaden the sweep of judicial discretion when interpreting laws that force consideration of difficult jurisprudential questions. The result is that it can often be difficult to know the effects of federal laws on state laws. Presumably, this provides a bulwark of stability in state laws.

[48] A particular kind of law's relative "quantumness" seems to bear very little relationship to the amount of democratic accountability or legitimacy it possesses. Considering the onerous (and often fruitless) process that must be undertaken to amend it, the Constitution is perhaps the least democratic of all American law, even when compared with the oft-assailed federal judiciary, which at least requires that judges be appointed and confirmed by democratically accountable branches. Of course, the Constitution makes up with legitimacy what it lacks in democratic responsiveness.

[49] This description may give short shrift to the pomp, as I have called it, of ratifying state constitutional law. This would not be fair of me to do without at least an acknowledgement of the widely different sets of practice implicated by the constitutional laws of different states. Although state constitutional law in many instances might be an exception to this observation, there are at least a couple of examples that support such a generalization. Many states allow for constitutional amendment through ballot initiative, which is as decentralized a way of making law as exists. *See State-by-State List of Initiative and Referendum Provisions*, INITIATIVE & REFERENDUM INST. AT THE UNIV. OF SOUTHERN CAL., http://www.iandrinstitute. org/statewide_i&r.htm (last visited Nov. 21, 2015). Moreover, states are smaller and more insular, and their electorates share more common interests and are divided by fewer cleavages. This may obviate the more difficult formal requirements in a way that is less likely to happen at the federal level.

examples do not occupy the entire field, and they certainly do not populate its outer bounds.

With a paper and pen, any two individuals can write a binding law as between themselves. A contract binds its signers as surely as any statute, albeit without the criminal statute's concomitant threat of punishment for violation.[50] In fact, even paper and pen are unnecessary if the contract does not trigger the Statute of Frauds.[51] And while a contract is—ostensibly, at least—a creature of individual consent, an agreement to be bound engages the state's legal apparatus and can impose limits on the legal relationships that others can enter into. But there remain certain trappings of formalism, especially in the formation of a contract.[52]

A contract must conform in all ways with each type of law described above.[53] It must also conform to the common law within the jurisdiction where enforcement is sought.[54] Beyond that, a contract is governed by its own internal rules: its duration, its objects, and the manner of its execution are all dictated—within the bounds permitted by higher-order laws—by its own terms. Myriad contracts are entered into every day—even the docks and clipboards are gone—and in as many places, and each contract carries the force of

[50] To be sure, however, this is not to say that violation does not bring to bear the state's coercive powers.

[51] U.C.C. § 2-201(1) (AM. LAW INST. & UNIF. LAW COMM'N 2002) (explaining that contracts for the sale of goods in excess of $500 require some form of writing).

[52] *See, e.g.*, RESTATEMENT (SECOND) OF CONTRACTS § 71 (AM. LAW INST. 1981) (describing the formal requirements of consideration).

[53] *See, e.g.*, RESTATEMENT (SECOND) OF CONTRACTS § 179 (AM. LAW INST. 1981) (describing bases of public policy against judicial enforcement of contracts). Note that a contract that "violates" the Constitution is not invalid per se, but a court cannot enforce a contract in such a way as to violate the Constitution. *Id.* Thus, the analysis is nearly identical to that of *Shelley v. Kraemer*. *See* Shelley v. Kramer, 334 U.S. 1, 10-14 (1948).

[54] *See, e.g.*, VA. CODE ANN. § 11 (2006) (listing contract requirements for the Commonwealth of Virginia). *See also*, Flores v. Am. Seafoods Co., 335 F.3d 904, 910 (9th Cir. 2003) (applying the parties' jurisdictional choice of law). Choice of law adds another wrinkle to this manner of "lawmaking." Though not the topic of this article, issues pertaining to contractual choice of law amplify the uncertainty associated with the legal ripples emanating outward from any contract, thus making such issues appropriate considerations in determining which end of the quantum spectrum a particular contract lies within.

law but somehow manages to escape even a hint of the epithet "simply self-refuting."

A similar analysis can be applied to property transactions. At the simplest level, a property transaction is a purely private affair, even when one of those private parties is a public entity like a state.[55] But if one accepts the well-worn adage that property is a bundle of legal rights,[56] then a property transaction reconfigures those rights by redefining the legal relationships between the parties and of the parties to the property. So we might say a property transaction changes the law as to its parties. Put another way, one can see property laws as canals through which legal rights flow, and a property transaction serves to reroute the canals that connect the parties and the property. Just as contract law allows parties to make binding law as between themselves, property law behaves similarly, especially where the transaction involves land with covenants running to it. And just as parties may not contract so as to violate the Constitution, federal law, state law, or the common law of their jurisdiction, so too are their covenants restricted by the entire panoply of laws that take precedence over the whims the parties would conscript the judiciary to uphold.[57] Under the rules of property law, the dock and clipboard are themselves up for grabs and the agreement of the parties—lacking even the formality of consideration—undoubtedly possesses the force of law. Again, it

[55] "[L]ike other associations and private parties, a State is bound to have a variety of proprietary interests. Alfred L. Snapp & Son, Inc. v. Puerto Rico, *ex rel.,* Barez, 458 U.S. 592, 601 (1982). A State may, for example, own land or participate in a business venture. As a proprietor, it is likely to have the same interests as other similarly situated proprietors." *ex rel., Barez*, 458 U.S. at 601.

[56] *See, e.g.*, Kaiser Aetna v. United States., 444 U.S. 164, 176 (1979) ("the bundle of rights that are commonly characterized as property . . .").

[57] *See, e.g.*, Shelley, 334 U.S. at 19-20. The Court in *Shelley* splits hairs over the legality of the covenant itself by technically proscribing only judicial enforcement of a constitutionally repugnant covenant. *Shelley*, 334 U.S. at 19-20. Chief Justice Vinson wrote that "judicial action is not immunized from the operation of the Fourteenth Amendment simply because it is taken pursuant to the state's common-law policy. Nor is the Amendment ineffective simply because the particular pattern of discrimination, which the State has enforced, was defined initially by the terms of a private agreement." *Id.* at 20 (footnote omitted). This quotation from *Shelley* is doubly illustrative in that it also demonstrates the relative position of the relevant common law on the quantum continuum.

seems Justice Souter left out something tacitly understood but quite important in his sweeping pronouncement.

C. Military Law

The relatively more quantum species of law described above are still familiar, despite the gradually increasing proliferation of "slits." These forms are fixed features in what we think of as the normal or traditional legal motif. Military law is, to the vast majority of Americans, significantly less familiar. Even seasoned jurists treat it as downright exotic. The Supreme Court itself has described military law with a deference approaching awe. "An army," wrote Justice Brewer for a unanimous court, "is not a deliberative body. It is the executive arm. Its law is that of obedience."[58] But this truism offers no help in understanding the nature of that unquestionably executive law. It leaves open questions of whether obedience is legal per se, and what manner of limits can operate on a commander's discretion to issue a directive. Justice Brewer elaborated but still left little room for these inquiries:

> No question can be left open as to the right to command in the officer, or the duty of obedience in the soldier. Vigor and efficiency on the part of the officer, and confidence among the soldiers in one another, are impaired if any question be left open as to their attitude to each other. So, unless there be in the nature of things some inherent vice in the existence of the relation [between the soldier and the army], or natural wrong in the manner in which it was established, public policy requires that it should not be disturbed.[59]

---

[58] United States v. Grimley, 137 U.S. 147, 153 (1890).

[59] *Grimley*, 137 U.S. at 153. *Grimley* centered about the court martial of John Grimley for desertion. *Id.* at 149. Grimley had falsified his enlistment, though, and had attempted to use this fact as a shield on the theory that he had never been enlisted at all and hence could not have deserted. *Id.* at 149-50. Justice Brewer's comment regarding "inherent vice in the existence of the relation" is a reference to the defect in Grimley's enlistment, which was nothing more than that he had claimed to be younger than he was in fact. *Id.* at 153. This did not amount to the sort of vice to which the Court referred, and it was thus insufficient reason in the eyes of the Court to disturb the relationship between Grimley and the Army that was premised on "the law . . . of obedience." *Id.* at 153-54.

Despite this almost mystical relationship of command and obedience described by the Court, it is well established that unreasonable obedience to an unlawful order is neither legal nor defensible.[60] Further, a commander's authority to govern his or her subordinates by fiat has definite limits. It is the sources of this authority to command by order and the contours of its constraints that truly define military law, and these features provide the context necessary for placing military orders along our quantum spectrum of legal activity.

1. The Uniform Code of Military Justice ("UCMJ")

At the highest level, a body of statutory law called the UCMJ governs the military.[61] Congress passed the UCMJ under its constitutional authority to "make Rules for the Government and Regulation of the land and naval Forces."[62] Beyond the UCMJ, there are numerous other statutes by which Congress exercises power over

[60] This has famously been described as the "Nuremberg defense," which provides that disobedience of some orders can be seen as not only lawful but as obligatory if the orders violate some higher-order law. *See* United States v. Huet-Vaughn, 43 M.J. 105, 114 (C.A.A.F. 1995) (explaining that the Nuremberg defense applies "only to individual acts committed in wartime . . . 'that constitute[] a crime . . . [leaving] no rational doubt of [] unlawfulness.'"). It is an affirmative defense to disobedience, and it is so named for the principle that those tried at Nuremberg should have disobeyed certain military orders because of duties arising under international law. *See, e.g.*, *Huet-Vaughn*, 43 M.J. at 114-15 (explaining that "[t]he duty to disobey an unlawful order applies only to 'a positive act that constitutes a crime' that is 'so manifestly beyond the legal power or discretion of the commander as to admit of no rational doubt of their unlawfulness.' ") (citing United States v. Calley, 22 C.M.A. 534, 543 (1973)). The standard in *Huet-Vaughn* is a steep one indeed, but its pedigree is unquestionable. Using language not at all unlike that of Justice Brewer in *Grimley* (but predating *Grimley* by more than two decades), Judge Deady in *McCall v. McDowell* enunciated the core concern with empowering soldiers with discretion to disobey their superiors' orders. The first duty of a soldier is obedience, and without this there can be neither discipline nor efficiency in an army. McCall v. McDowell, 15 F. Cas. 1235, 1240 (C.D. Cal. 1867). One might ask whether this leaves a gap sufficient for even the narrow edge of the *Huet-Vaughn* standard.

[61] *See generally* Uniform Code of Military Justice, 10 U.S.C. Subt. A, Pt. II, Ch. 47. The Constitution itself provides some degree of even more fundamental law governing the military. *See, e.g.*, U.S. CONST. amend. III. But the Constitution is strictly classical in nature, which means a discussion of these provisions would add very little to this discourse.

[62] U.S. CONST. art. I, § 8, cl. 14.

the military.[63] But the UCMJ is the basic kernel of military law in that it sets forth the relationship between the service member and all other military law, and its edicts form an essential part of every service member's basic military education.[64]

Many provisions of the UCMJ are quite specific. The UCMJ prescribes strictures for many kinds of personal and professional conduct, with prohibitions against such sundry offenses as sodomy,[65] misbehavior before the enemy,[66] absence without leave ("AWOL"),[67] mutiny,[68] malingering,[69] and dueling.[70] The UCMJ also defines and proscribes common criminal offenses such as rape,[71] assault,[72] murder,[73] and arson.[74] It also carefully circumscribes the sorts of proceedings (both judicial—i.e., court-martial[75]—and non-judicial[76]) that are appropriate for adjudicating alleged violations of the UCMJ's punitive articles, and the sentences that may be awarded upon conviction.[77]

---

[63] *See, e.g.*, Department of the Army, Organization, 10 U.S.C. § 3011 (providing that the Department of the Army is organized under the Secretary of the Army).
[64] *See, e.g.*, U.S. ARMY TRAINING AND DOCTRINE COMMAND, INITIAL ENTRY TRAINING SOLDIER'S HANDBOOK (2008), http://www.tradoc.army.mil/tpubs/pams/p600-4.pdf.
[65] Forcible Sodomy; Bestiality, 10 U.S.C. § 925 (1956).
[66] Misbehavior Before the Enemy, 10 U.S.C. § 899 (1956).
[67] Absence Without Leave, 10 U.S.C. § 886 (1956).
[68] Mutiny or Sedition, 10 U.S.C. § 894 (1956).
[69] Malingering, 10 U.S.C. § 915 (1956).
[70] Dueling, 10 U.S.C. § 914 (1956).
[71] Rape and Sexual Assault Generally, 10 U.S.C. § 920(a) (1956).
[72] Assault, 10 U.S.C. § 928 (1956).
[73] Murder, 10 U.S.C. § 918 (1956).
[74] Arson, 10 U.S.C. § 926 (1956).
[75] *See* Courts-Martial Classified, 10 U.S.C. § 816 (1956).
[76] *See* Commanding Officer's Non-Judicial Punishment, 10 U.S.C. § 815 (2002). Non-judicial punishment ("NJP") is a less formal adjudicatory option that is available to commanding officers when dealing with alleged offenses by members of their commands. But someone accused in such a proceeding can demand a trial by court-martial unless attached to an embarked vessel. Although less formal, NJP is a legal proceeding, and "awards" at NJP can include correctional custody, extra duties, demotion, forfeiture of pay, and "confinement on bread and water . . . for not more than three consecutive days." 10 U.S.C. § 815(b)(2)(A) (2002).
[77] *See* 10 U.S.C. §§ 855-58b (approved 2015).

Among the UCMJ's punitive articles, there are also several broadly defined substantive offenses that are unique to the customs and traditions of the military. For instance, "conduct unbecoming an officer and a gentleman" is punishable if committed by a commissioned officer or a candidate for commission.[78] Additionally, the UCMJ's "General Article" covers any residual offenses not mentioned. It forbids "all disorders and neglects to the prejudice of good order and discipline in the armed forces, all conduct of a nature to bring discredit upon the armed forces, and crimes and offenses not capital."[79] Beyond these "catch-all" provisions, there are also punitive articles that delegate legal authority over subordinates to superiors. Article 90 makes willful disobedience of any superior commissioned officer an offense punishable by death in time of war and at any other time by "such punishment, other than death, as a court-martial may direct."[80] Article 91 extends this offense to the willful disobedience of a lawful order given by "a warrant officer, noncommissioned officer, or petty officer."[81] Finally, article 92 provides for punishment of violating or failing "to obey any lawful general order or regulation," as well as knowingly failing to obey "any other lawful order issued by a member of the armed forces, which it is his duty to obey."[82] As noted above, the fact that these articles make the failure to obey lawful orders punishable as substantive offenses has the effect of legal delegation.

2. Delegation of Military Authority Beyond the UCMJ

Once past the statutory framework that Congress has furnished to govern and regulate the military, it is delegation all the way down. The President is designated the commander in chief of

[78] Conduct Unbecoming an Officer and a Gentleman, 10 U.S.C. § 933 (1956).
[79] General Article, 10 U.S.C. § 934 (1956).
[80] Assault or Willfully Disobeying Superior Commissioned Officer, 10 U.S.C. § 890 (1956).
[81] Insubordinate Conduct Toward Warrant Officer, Noncommissioned Officer, or Petty Officer, 10 U.S.C. § 891 (1956) (extending only punishments other than death to willful disobedience offenses). This article also criminalizes contemptuous and disrespectful behavior toward warrant officers, noncommissioned officers, and petty officers. 10 U.S.C. § 891(2) (1956).
[82] Failure to Obey Order or Regulation, 10 U.S.C. § 892 (1956). This article also defines as a substantive offense dereliction in the performance of duties.

the armed forces by the Constitution,[83] and Congress has specifically authorized the President to "prescribe regulations to carry out his functions, powers, and duties" relating to military affairs.[84] It is not entirely clear how much daylight, if any, exists between the powers delegated to the President by the Constitution and those delegated by Congress.[85] Indeed, considering the Supreme Court's view of the commander in chief power, the statutory authorization might have little more significance than an approving nod by Congress.[86]

[83] U.S. CONST. art. II, § 2, cl. 1. *See, e.g.*, United States v. Eliason, 41 U.S. 291, 301 (1842) ("[t]he power of the executive to establish rules and regulations for the government of the army, is undoubted.").

[84] Regulations, 10 U.S.C. § 121 (1956). Congress has by statute also authorized the President to prescribe regulations for the Army (Department of the Army: Regulations, 10 U.S.C. § 3061 (1956)) and Air Force (Department of the Air Force: Regulations10 U.S.C. § 8061 (1956)), as well as in a few other specific capacities. It is difficult to imagine what work these authorizations do that 10 U.S.C. § 121 does not, but Congress has nonetheless seen fit to at least voice its acquiescence to the exercise of such power from time to time. *See generally* 6 C.J.S. *Armed Services* § 25 (2015) (describing the President's commander-in-chief powers).

[85] Historically the President and other members in the chain of command were considered to have regulatory power only insofar as such power was confined to executive prerogatives. WILLIAM WINTHROP, MILITARY LAW AND PRECEDENTS 33-34 (2d ed. 1920). Though now disfavored, the doctrine of nondelegation was long considered fundamental to understanding the contours of executive authority to regulate the military. "A regulation which assumes to prescribe in regard to a matter which is properly the subject for original legislation, departs from 'the range of purely executive or administrative action,' is in a just sense a regulation no longer, and can have no legal effect as such." *Id.* at 33 (footnote omitted) (quoting 6 ROBERT FARNHAM, OFFICIAL OPINIONS OF THE ATTORNEYS GENERAL OF THE UNITED STATES 15 (1856)). However, it is an open secret that the distinction between executive regulatory power and constitutionally defined legislative power is largely illusory. *See*, *e.g.*, Whitman v. Am. Trucking Associations, 531 U.S. 457, 488 (2001) (Stevens, J., concurring).

[86] *See, e.g.*, Free Enter. Fund v. Pub. Co. Accounting Oversight Bd., 130 S. Ct. 3138, 3160 (2010) ("[m]ilitary officers are broadly subject to Presidential control through the chain of command and through the President's powers as Commander in Chief."). One possible explanation is that Congress, like the Court, is more concerned with the potential for turning the military into a "debating school" than with granting to the President too much discretion in matters concerning the regulation of the military. In that case, it might be Congress's intent to provide the President with the benefit of a unified command voice by preemptively placing the President's power at its zenith. As Justice Jackson put it in *Youngstown Sheet & Tube Co. v. Sawyer*, "[w]hen the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum, for it includes all that he

Nevertheless, both forms of delegation obtain, and either is sufficient in itself to allow the President to make rules governing the military.[87]

The President has the authority to delegate his own powers to certain officers chosen "with the advice and consent of the Senate."[88] Congress has also delegated, subject to Presidential approval, rulemaking authority over the military to the Secretary of Defense,[89] to a host of deputies and undersecretaries,[90] and to the secretaries of each military branch over their respective components.[91] Then, operating under the "authority, direction, and control" of their respective secretaries, the staff offices of the Military Service Chiefs are empowered to develop plans for "recruiting, organizing, supplying, equipping. . . training, servicing, mobilizing, demobilizing, administering, and maintaining" their departments and providing "detailed instructions for the execution of the approved plans and supervis[ing]" their implementation.[92] But while the Service Chiefs are technically the military's highest-ranking commissioned officers, the Combatant Commanders enjoy effective operational "authority, direction, and control"—subject only to direction by the President and Secretary of Defense—over the vast Combatant Commands they head.[93]

---

possesses in his own right plus all that Congress can delegate." Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 635 (1952) (Jackson, J. concurring).

[87] Note, however, that such rules are at least one, and perhaps two, steps away from the classical bedrock of the Constitution. *See, e.g.*, *Youngstown*, 343 U.S. at 635-39.

[88] General Authorization to Delegate Functions; Publication of Delegations, 3 U.S.C. § 301 (1951).

[89] Secretary of Defense, 10 U.S.C. § 113 (2014) (narrowly defining the authority delegated to the Secretary of Defense, absent delegation from the President).

[90] *See generally* 10 U.S.C. §§ 131-44 (1956) (creating the Deputy Secretary of Defense, 14 Assistant Secretaries, Inspector General, Director of Operational Test and Evaluation, General Counsel, ODS personnel, Director of Small Business Programs, and Under Secretaries of Defense for Acquisition, Policy, Comptroller, Personnel and Readiness, Intelligence, and Chief Information Officer).

[91] 10 U.S.C. §§ 3013, 5013, 8013 (1956). Similar authority exists for the Secretary of Homeland Security over the Coast Guard (14 U.S.C. § 633 (1949)).

[92] *See* 10 U.S.C. §§ 3032, 5032, 8032 (1986). The Military Service Chiefs occupy extremely influential positions, they do not exercise operational command over their services.

[93] Commanders of Combatant Commands: Assignment; Powers and Duties, 10 U.S.C. § 164 (2008). A Combatant Command is either a Unified Combatant

3. Delegation of Military Authority As a Gap Filler

Further down the authority to regulate the military goes. But let's return now to those three delegative articles—10 U.S.C. sections 890, 891, and 892. As noted above, the UCMJ enumerates the failure to obey a general order as a substantive offense,[94] but the UCMJ does not define the term "general order." Nor does the UCMJ define who has the authority to promulgate such orders. These gaps have been filled in by accretion; military case law constitutes a common law of its own, and, "to maintain the discipline essential to perform its mission effectively, the military has developed what 'may not unfitly be called the customary military law' or 'general usage of the military service.'"[95] Regarding general orders, this usage is distilled in the United States Manual for Courts Martial, which states:

> General orders or regulations are those orders or regulations generally applicable to an armed force which are properly published by the President or the Secretary of Defense, of Homeland Security, or of a military department, and those orders or regulations generally applicable to the command of the officer issuing them throughout the command or a particular subdivision thereof which are issued by: (i) an officer having general court-martial jurisdiction; (ii) a general

---

Command or a Specified Combatant Command. *See* 10 U.S.C. § 161 (2011). A Unified Combatant Command is defined by statute as "a military command which has broad, continuing missions and which is composed of forces from two or more military departments." 10 U.S.C. § 161. A Specified Combatant Command is "a military command which has broad, continuing missions and which is normally composed of forces from a single military department." *Id.* These are often massive commands and include such newsworthy names as CENTCOM, PACOM, and the newly inaugurated AFRICOM. *See generally*, *About U.S. Central Command (CENTCOM)*, U.S. CENT. COMMAND, http://www.centcom.mil/en/ about-centcom (last visited Dec. 7, 2015).

[94] 10 U.S.C. § 892 (1956).

[95] Parker v. Levy, 417 U.S. 733, 744 (1974) (quoting Martin v. Mott, 25 U.S. 19, 35 (1827)). *See also* WINTHROP, *supra* note 85, at 17 ("[m]ilitary law proper is that branch of the public law which is enacted or ordained for the government exclusively of the military state, and is operative equally in peace and in war…Like [civil] law, it consists of a Written and an Unwritten law.").

> or flag officer in command; or (iii) a commander superior to (i) or (ii).[96]

This imposes a qualitative limit on who can issue these very rule-like orders, but it imposes no quantitative ceiling.[97] In fact, the President and the secretaries of the various military departments are authorized to designate "any. . . commanding officer" as having general court-martial jurisdiction, so the only limits are the number of commanding officers and the executive's policy choices regarding how widespread the authority ought to be.[98] This is a large pool from which to choose. The upshot is that "general orders and regulations," which bear all the hallmarks of a legislative rule, can be "churned out" at an astonishing rate at literally hundreds of commands around the globe.[99] When combined with the "law of obedience," one cannot help but notice the ever-advancing territory of the "self-refuting" proposition that vexed Justice Souter in *Mead Corp*.[100]

But the sheer promiscuity of this rulemaking authority is hardly its most shocking feature. The rules promulgated within the military do not govern only issues of "national security." Few organizations are as purely bureaucratic as the military,[101] so it

---

[96] MANUAL FOR COURTS-MARTIAL, UNITED STATES pt. IV-23, ¶ 16.c.(1)(a) (2008) [hereinafter MCM].

[97] This is not, however, no limit at all. The authority to convene courts-martial is nondelegable; those who possess such authority do so from its source, and those not empowered by this font of authority cannot otherwise receive it. *See* 10 U.S.C. § 113 (2011); MCM, *supra* note 96, at II-48, R.C.M. 504(b)(4).

[98] Who May Convene General Courts-Martial, 10 U.S.C. § 822 (2006).

[99] And the reach of this jurisdiction is unquestionably global. The UCMJ's provision for extraterritoriality is sublimely succinct: "This chapter applies in all places." Territorial Applicability of this Chapter, 10 U.S.C. § 805 (1980).

[100] United States v. Mead Corp., 533 U.S. 218, 233-34 (2001).

[101] Max Weber, a celebrated sociologist and early organizational behavior theorist, famously enumerated "six features that characterize a bureaucracy: (1) it covers a fixed area of activity, which is governed by rules; (2) it is organized as a hierarchy; (3) action that is undertaken is based on written documents (preserved as files); (4) expert training is needed, especially for some; (5) officials devote their full activity to their work; and (6) the management of the office follows general rules which can be learned." RICHARD SWEDBERG & OLA AGEVALL, THE MAX WEBER DICTIONARY 19 (2005) (citing MAX WEBER, ECONOMY & SOCIETY (1922)). These criteria also characterize the military.

should come as little surprise that many of the rules governing the military are primarily bureaucratic in nature. Office policies, safety procedures, grooming standards, and dress codes are just a few of the categories of rules that apply generally to command personnel. And provided such policies and standard operating procedures ("SOPs") are reasonably understood as implicating disciplinary consequences (i.e., "punitive orders"),[102] their resemblance to the law as defined by Black's is uncanny: these rules are applied systematically; they apply to military society (and are accepted by society at large); and they are backed by the threat of coercive force.[103]

D. The Informality of Military Law

The military's rulemaking and enforcement authority stands in contrast to managerial policies in other executive agencies. Absent another substantive legal violation, agency SOPs and office policies do not ordinarily bind employees such that they face criminal liability. At most, low-level bureaucrats are typically subject to no

[102] "[I]f a regulation does not contain language establishing that it is a punitive regulation, a violation of the regulation is not a criminal offense. . . ". United States v. Shavrnoch, 49 M.J. 334, 336 (C.A.A.F. 1998). *See also* United States v. Hughes, 48 M.J. 214, 217 (C.A.A.F. 1998) ("[a]ny ambiguity in construing a punitive regulation should be resolved in appellant's favor.").

[103] It should be understood that military personnel with the authority to order subordinates do not have carte blanche. Orders that are "broadly restrictive of private rights must have some connection to military need." 57 C.J.S. *Military Justice* § 83 (2015). Thus, the specific elements of a lawful order or regulation are: "(1) issuance by competent authority – a person authorized by applicable law to give such an order; (2) communication of words that express a specific mandate to do or not do a specific act; and (3) relationship of the mandate to a military duty." United States v. Deisher, 61 M.J. 313, 317 (C.A.A.F. 2005). Relationship to military duty has, however, been interpreted quite broadly. *See, e.g.*, United States v. Lugo, 54 M.J. 558, 559 (N-M. Ct. Crim. App. 2000) (holding a general order prohibiting Marines from wearing earrings while off-duty and in civilian attire sufficiently related to military conduct to constitute a lawful order); Goldman v. Weinberger, 475 U.S. 503, 503 (1986) (holding a general order forbidding the wearing of yarmulkes in uniform to be lawful). Additionally, a properly issued general order is presumed to be lawful, and the accused violator bears the burden of demonstrating the unlawfulness of the order. United States v. Hughey, 46 M.J. 152, 155 (C.A.A.F. 1997).

worse than disciplinary termination.[104] But even if egregious lapses coupled with a related criminal offense might result in harsher forms of discipline, it is unthinkable that they might result, in and of their own force, in incarceration, let alone a three-day stint of subsistence on bread and water. Put simply, office rules outside the military context are not backed by force, so they fall short of our working definition of law.

In fact, it is not even clear that agencies themselves will be bound by their internal policies. Falling under the APA's rubric of "interpretative rules, general statements of policy, or rules of agency organization, procedure, or practice," internal agency rules do not go through the same process as "legislative" rules, and courts have been reluctant to find in them binding legal force.[105]

By contrast, for the military, which is not subject to the procedural rigors of the APA,[106] properly formulated general orders and regulations governing a military unit's "organization, procedure, or practice" have the force of law, and subject service members ignore those laws at their own peril.[107]

---

[104] *See generally* U.S. MERIT SYSTEMS PROTECTION BOARD, WHAT IS DUE PROCESS IN FEDERAL CIVIL SERVICE EMPLOYMENT? (May 2013) (describing in detail the disciplinary penalties and procedures for federal civil service employees).

[105] *See* Nina A. Mendelson, Agency Burrowing: Entrenching Policies and Personnel Before A New President Arrives, 78 N.Y.U. L. REV. 557, 666 n.71 (2003).

[106] *See* Rule Making, 5 U.S.C. § 553(a)(1) (1978) (exempting from rulemaking procedures those matters involving "military or foreign affairs function[s] of the United States").

[107] 5 U.S.C. § 553(b)(3)(A) (1978). Though dated, Colonel Winthrop's analysis of the lawfulness of military regulations fleshes the concept out nicely. "It is indeed somewhat loosely said of the army regulations by some of the authorities that they have 'the force of law,' but this expression is well explained by the court in U.S. v. Webster, as follows: 'When it is said that they have the force of law, nothing more is meant than that they have that virtue *when they are consistent with the laws established by the Legislature*.' That is to say, while they have a legal force, it is a force quite distinct from, and inferior and subordinate to, that of the statute law." (footnotes omitted) (emphasis added). WINTHROP, *supra* note 85, at 32 (quoting United States. v. Webster, 28 F. Cas. 509, 515 (D. Me. 1840)). Colonel Winthrop thereby establishes the legal obligation residing in military regulations while simultaneously noting the precarious position it occupies with respect to its superior law.

Even general orders promulgated in this fashion bear enough resemblance to other administrative rules that their increasingly quantum nature might not be unsettling. These "laws" are subject to ever more intricate legal constraints as they occupy ever-lower strata in the legal hierarchy. But general orders also affect a relatively small group of individuals. And the more a general order or regulation is susceptible to invalidation by the levels of law rising above it, the smaller the group of affected individuals grows.

The UCMJ's delegative articles do not stop at the level of general orders and regulations, and the correlation between smaller effective delegations of legal authority and increasing quantum uncertainty persists. Any military member of pay grade E-4 or above is endowed by the UCMJ with the authority to issue orders to their subordinates.[108] As with general orders and regulations, failure to obey these orders can result in criminal liability.[109] And, as with general orders and regulations, much of what transpires in the form of direct orders amounts to little more than office management. Nevertheless, the temptation to dismiss the notion that seemingly insignificant orders are "law" simply because they most often contemplate the mundane should be resisted. The workaday nature of many lawful direct orders stands in stark contrast to the most highly dynamic subset of such orders that occur on the battlefield.

With each successively more quantum form of lawmaking, the formality required decreases accordingly. To pass a statute that is

---

[108] 10 U.S.C. § 891 (1956). There is an exception to this statement as I have formulated it. By a quirk of ranking structure, the Army employs some E-4 service members who are not noncommissioned officers; these are Specialists, and they typically work in technical fields. All members from the pay grade of E-5 and above are considered noncommissioned officers. *See generally*, *Enlisted Army Ranks*, MILITARY.COM, http://www.military.com/army/enlisted-ranks.html (last visited Dec. 21, 2015).

[109] *See, e.g.*, 10 U.S.C. § 890 (1956). But an order not to commit another substantive offense under the UCMJ is preempted by the other substantive offense. Thus, an order not to violate another punitive article cannot result in charges both for the underlying conduct and for the failure to obey the order. *See, e.g.*, United States v. Curry, 28 M.J. 419, 424 (C.M.A. 1989) ("[a]rticle 93, the punitive article which proscribes maltreatment of subordinates, preempted the conviction under Article 92 for disobedience of an order not to maltreat subordinates.").

subordinate only to the Constitution and that constitutes "the Supreme Law of the Land," [110] Congress must fulfill its constitutionally required procedures and navigate an obstacle course of internally created procedural rules. [111] To pass a generally applicable rule governing enormous swaths of American life and industry, an executive agency must, at the very least, undertake the years-long process of "informal" rulemaking, [112] which includes publication of the proposed rules and opportunity for interested parties to comment on the proposal, and the agency must respond to all major comments received.[113] Even following these formalities, statutes and regulations are nearly always subject to judicial review, provided they meet all requirements of justiciability. Military regulations governing a multi-million-volunteer fighting force, which spring from some combination of legislative delegation and the black box of intra-executive power, can be promulgated without resort to the APA.[114] General orders (other than those issuing from the uppermost reaches of the military's civilian leadership) require only promulgation by a properly designated commanding officer or other high-ranking officer.[115] An especially forward service member might challenge a general order or regulation, but typically only after having already run afoul of it. Finally, with direct orders from commissioned officers, warrant officers, noncommissioned officers, and petty officers, nearly all formality is stripped away. The ordering supervisor's rank and a clear statement that her full authority is being

[110] U.S. CONST. art. VI, cl. 2.
[111] U.S. CONST. art. I, §§ 5, 7.
[112] *See* 5 U.S.C. § 553 (1978) (providing for a number of exceptions, including the unctuously titled "good cause exception.") In order to issue a "legally binding norm," an agency must go through the formalities prescribed by the APA. *Id.*
[113] *See* United States v. Nova Scotia Food Corp., 568 F.2d 240, 249 (2d Cir. 1977) (interpreting 5 U.S.C. § 553 (1978) as requiring a reasonably developed record, including the data relied on by the agency and responses to pertinent questions from the public).
[114] 5 U.S.C. § 553(a)(1) (1978).
[115] *See* 10 U.S.C. § 892(1) (2015); MCM, *supra* note 96, at PT. IV, ¶ 16b. Note that no knowledge of the order is required. Neither, for that matter, is there a requirement that a service member reasonably should have known of the existence of a properly promulgated order. Promulgation includes publication, which presumably serves the purpose of giving notice to those subject to the order. But just as ignorance of the law is no defense, neither is ignorance of a lawful general order. *See* 10 U.S.C. § 892(1) (2015); MCM, *supra* note 96, at PT. IV, ¶ 16b.

invoked by the order are sufficient to satisfy the procedural requirements. And a challenge to such an order, absent a showing such as that required in *Huet-Vaughn* (that is, that the order is manifestly unlawful beyond any rational doubt),[116] must almost certainly come only after it has been obeyed. Nowhere is this truer than on the field of battle.

Combat footage from Fallujah on the Internet illustrates the two basic kinds of communication one is likely to encounter on a battlefield: operational information flowing both up and down the chain of command, and orders flowing exclusively down.[117] As to the former, soldiers on the ground continuously relay information about their surroundings to one another. The need for this kind of communication in combat is self-evident. But a combat unit is not run according to an abstract egalitarian ideal. It is not a committee. So although information flows omnidirectionally, the other form of communication does not: orders radiate from those with higher rank or positional authority to those with lower rank or positional authority. And if you watch enough of this footage, you will notice other patterns that emerge. Combat happens quickly. It is dynamic. It is chaotic. But the communication is fluid. It is seamless. Amid a flurry of "get out of here!" and "go, go, GO!" and "get up on the roof!" you will not find a "but" or a "why?" And this is probably how it should be. But that does not tell us what the law is doing in such a perilous environment.

In such environments, the delegative power conferred by the UCMJ is at its peak. This is attributable to more than just the unquestioned "right to command in the officer, or the duty of obedience in the soldier," although it is both.[118] It is law. And a soldier is not permitted the time to check an order against a table populated by all the international and domestic laws potentially

---

[116] *See, e.g.*, United States v. Huet-Vaughn, 43 M.J. 105, 114-15 (C.A.A.F. 1995).
[117] *See*, *e.g.*, Avidanofront, *Iraq Fallujah – Intense Combat Footage Straight from the Frontlines*, YOUTUBE (Sept. 2, 2013), https://www.youtube.com/watch?v=hHr48aEhQh8&oref=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3DhHr48aEhQh8&has_verified=1(graphic content).
[118] *See id.*

implicated by an order. Hence, even if unlawful, to the soldier the order is law.

On the field of battle, uncertainty is so different in amount as to also be different in kind. Not only are these orders subject—in practice, of course, only ex post facto—to a multitude of higher-order laws to which they must conform, but they are also based on rapidly changing contemporaneous information. Whereas the legislative and regulatory processes typically allow for a leisurely influx of information, and even direct orders in an office environment can be issued as time permits (as in a memo or email), battlefield orders are affected by events immediately preceding them, and they will affect events that immediately follow. Even the speed with which informal adjudications sort claims into denied and approved piles does not approach the rapidity with which combat orders must issue. In other words, if normal law has a quantum character that is comparable to the releasing and eventual observation of individual photons, battlefield orders are more like the splashes of undifferentiated light: they come in waves.

E. Interactivity of Orders

The issue of how orders interact (and with what) is also important. Laws change circumstances to which they are addressed. Sometimes multiple laws affect the same objects, or a single law affects multiple facets of society. But the point is that laws tend to interact with one another. In the regulatory setting, it is not difficult to imagine how rules relating to water treatment might affect rules about agricultural water use, which might in turn interact with rules about cattle ranching, and so on.

Another, adversarial form of interaction occurs in the making and enforcing of laws. Some laws contemplate their own violation *ex ante*.[119] And while regulatory laws are crafted in part with the violator in mind, criminal law perfectly instantiates the notion that the law must impose consequences for its breach.

[119] This is, of course, the case with any law that prescribes a penalty. *See, e.g.*, Mitigating and Aggravating Factors to be Considered in Determining Whether a Sentence is Justified, 18 U.S.C. § 3592 (2006).

Criminal law focuses almost exclusively on its own violation, so one could say it is a body of law crafted in response to its enemy. The citizenry, to whom law should ideally be responsive, have directed the legislator, the prosecutor, and the judge to keep us safe by being "tough on crime." Criminal law thus embodies a fitful, slow-motion version of the battlefield calculus: the "good guys" know the "bad guys" are out there; they respond—either proactively or reactively—to what the "bad guys" do; and when the enemy adapts and responds, the soldier responds to that, too.[120] Hence, instead of laws that are ploddingly responsive primarily to the citizenry and its other "stakeholders" (e.g., regulated entities), battlefield orders are rapid-fire and unpredictable matters literally of life or death, and they respond primarily to an enemy whose interests are counter to those of the ordering commander's own nation.

In sum, the outer limits of the group of phenomena constituting lawful military orders are an expanse unlike any other area of law. Erupting from and informed by the vagaries of combat, lawful orders bind with all the force of any law (and more force than most),[121] albeit typically for only a few individuals and for only brief periods. Lawful orders are creatures of uncertainty; they cannot be lawful save by deftly avoiding conflict with the complex of laws superior to them in stature, but they can almost never be found unlawful (or confirmed as lawful) until after the fact. Moreover, as these bursts of lawmaking activity arise, they become entangled with other orders—of both friend and foe—in a web of interference, not unlike the chaotic interaction of ripples resulting from a fistful of

[120] Of course, the enemy on the battlefield is not, strictly speaking, breaking these laws. Rather, the enemy is likely to be operating in very similar ways such that enemy combatants are themselves enmeshed in webs of quantum lawmaking. This is decidedly less likely with "unconventional" enemies, but in either event, the "violation" that this law contemplates and responds to is countervailing quantum law. Disobeying a lawful battlefield order would be the actual violation, and the analysis of how such breach fits into the legal process involved is indistinguishable from that relating to criminal law above. *See, e.g.*, 10 U.S.C. § 890(2) (1956).

[121] Indeed, lawful orders given in time of war can be enforced with the harshest punishment available to the law. *See id.* (providing for the death penalty in the event of assaulting or willfully disobeying a superior commissioned officer in times of war). Thus, this is law's extremity in more ways than one.

pebbles being thrown into pond. If some law is deserving of the quantum metaphor, this is it.

This species of law is a far cry from the customs rulings in *Mead Corp*. In fact, attributing legal force to classifications "churned out" at 46 widely scattered brick-and-mortar customs offices can seem almost mundane in comparison. Even sausage making begins to seem a civilized and tidy endeavor. Nevertheless, the Court has held that—for whatever reason—customs rulings so promulgated do not have the force of law,[122] whereas the legal force of military orders is beyond serious cavil. But given their exotic nature, it is all the more important to examine the legal issues that lawful orders implicate.

II. THE LAW OF MILITARY LAW

In his seminal treatise on military law, Colonel William Winthrop had this to say of military regulations:

> To the student, as well as in practice, army regulations are the most unsatisfactory element of our written military law. Presented in connection with statutes from which they are sometimes imperfectly discriminated; not infrequently themselves partaking of the character of legislation and thus of doubtful validity; and fatally subject, as we have seen, to constant and repeated modification, their effect too often is to embarrass and mislead where they should assure and facilitate. . . . [T]hey should, in the opinion of the author, be reduced to the smallest available bulk; all that are really statutes and all that are of a legislative quality should be eliminated; only those should be included that are purely *general*. . . ; and the authority to amend should be most rarely exercised.[123]

In this single paragraph, Winthrop touched on many features of what I have called the quantum character of military regulation. To be sure, some of his concern is outdated. Winthrop wrote when the nondelegability of the legislative power was virtually

[122] United States v. Mead Corp., 533 U.S. 218, 233-34 (2001).
[123] WINTHROP, *supra* note 85, at 35-36 (footnote omitted) (emphasis in original).

unquestioned orthodoxy. So he found statute-like military regulations particularly suspect. But even as a manifestation of unadulterated executive power, this career military officer describes military regulations with a certain mistrust or unease.[124]

Despite the dust being long settled on the nondelegation doctrine,[125] the issue remains pertinent in the context of military law. Administrative law is undeniably legislative, no matter how one might cling to the Court's soothing "quasi-legislative" gloss.[126] And

[124] Given Winthrop's now-anachronistic view of the supposedly insuperable barrier between executive and legislative power, it is worth a moment's thought as to what is meant by the former. If there is such a thing as unadulterated executive power, instances of it are rare. Absent any kind of regulation or systematized interpretation, the main executive functions can likely be enumerated on a single hand: disbursement and collection; investigation, prosecution, and punishment of crime; intelligence gathering and the conduct of war; diplomacy; perhaps a few others. For Winthrop, even those regulations that govern only the military are invalid if too legislative in character. It is because this understanding ignores the necessary discretionary incidents of executive power that the Supreme Court eventually found a rigid nondelegation doctrine unworkable. *See, e.g.,* J. W. Hampton, Jr., & Co. v. United States, 276 U. S. 394, 406 (1928) ("[i]n determining what [Congress] may do in seeking assistance from another branch, the extent and character of that assistance must be fixed according to common sense and the inherent necessities of the government coordination."). Be that as it may, a strain of it seems still to apply to the military. Rather than concede that much of what governs the military exclusively from within the Executive Branch is legislative in character, there is a tendency to mystify the executive power in this context and fancy it imbued with an authority *sui generis*. *See*, *e.g.*, United States v. Grimley, 137 U.S. 147, 153 (1890). If legal governance of the military from within "the executive arm" were really such an impenetrable article of faith, then this examination would be unnecessary. *See Grimley*, 137 U.S. at 153. It would also be no more satisfying to the enquiring mind than other dogmas of metaphysics.

[125] *See*, *e.g.*, Elena Kagan, *Presidential Administration*, 114 HARV. L. REV. 2245, 2364 (2001) ("[i]t is, after all, a commonplace that the nondelegation doctrine is no doctrine at all."); Cass R. Sunstein, *Nondelegation Canons*, 67 U. CHI. L. REV. 315, 322 (2000) ("[w]e might say that the conventional [nondelegation] doctrine has had one good year, and 211 bad ones (and counting).").

[126] Justice Stevens, for one, has advocated abandoning this pretense. "We could . . . conclude that the delegation is constitutional because adequately limited by the terms of the authorizing statute. Alternatively, we could pretend, as the Court does, that the authority delegated to the EPA is somehow not 'legislative power.'…I am persuaded that it would be both wiser and more faithful to what we have actually done in delegation cases to admit that agency rulemaking authority is 'legislative

much of the law within the corpus of military regulation is "not infrequently . . . partaking of the character of legislation," as well.[127] The question, then, is from where this authority arises.

As mentioned above, fundamental authority over the military is a thing divided by the text of the Constitution itself.[128] According to the current state of affairs with the nondelegation doctrine, Congress can delegate its legislative authority over the military (or any other legislative authority, for that matter) to the executive branch provided it has enunciated an "intelligible principle" to guide the delegation.[129] Whether an intelligible principle is also necessary to guide the delegation of executive authority within the executive branch is less clear. The doctrine itself is premised on an inability of one branch to confer on another the powers granted to it by the Constitution. But the divide between those regulations that are legislative in character and those that are "simply . . . executive, administrative, instrumental rules and therefore distinguished from statutory enactment" is poorly defined,[130] so it is difficult to generalize too broadly. Despite these uncertainties, the traditional view is that the

> authority for army regulations proper is to be sought—primarily—in the distinctive functions of the President as Commander-in-chief and as Executive. His function as Commander-in-chief authorizes him to issue, personally or through his military subordinates, such orders and directions as are necessary and proper to ensure order and discipline in the army.[131]

power.'" Whitman v. Am. Trucking Associations, 531 U.S. 457, 488 (2001) (Stevens, J., concurring) (footnote omitted).

[127] WINTHROP, *supra* note 85, at 35-36.

[128] U.S. CONST. art. I, § 8, cl. 14; U.S. CONST. art II, § 2, cl. 1.

[129] J.W. Hampton, Jr., & Co. v. United States, 276 U.S. 394, 409 (1928) ("[i]f Congress shall lay down by legislative act an intelligible principle to which the person or body authorized to [exercise legislative power] is directed to conform, such legislative action is not a forbidden delegation of legislative power.").

[130] WINTHROP, *supra* note 85, at 32 (footnote omitted).

[131] *Id.* at 27 (footnote omitted).

Whether necessary or not, an intelligible principle of sorts emerges from this view.

Winthrop's words echo in those of the UCMJ's General Article ("all disorders and neglects to the prejudice of good order and discipline").[132] Rules to effectuate "order and discipline," then, lie within the breadth of the President's power to regulate (and to delegate).[133]

But there remains a question whether this principle is sufficiently intelligible to justify such delegations as Congress expressly granted. The UCMJ's punitive articles delegating the authority to issue orders to subordinates are statutory law. As discussed above, the orders they empower can cascade beyond mortal powers of prediction. Whether an intelligible principle can survive this atomization whereby lawful orders are issued and passed on again is a subject the courts have not specifically addressed.[134]

One possible concern with allowing delegation at progressively lower levels is that it shifts the risk associated with lawful actions further and further down the chain of command. If a subordinate carries out an unlawful order, that subordinate cannot escape liability simply by pointing a finger up the chain of command.[135] If an order is lawful but a subordinate finds it questionable, the subordinate can be punished for failure to obey. Only where the subordinate correctly discerns that the order is unlawful *and* refuses to obey can she escape liability.[136] As suggested

---

[132] 10 U.S.C. § 934 (1956).

[133] WINTHROP, *supra* note 85, at 27.

[134] However, the Supreme Court has generally afforded substantial deference to the judgment of military commanders. *See, e.g.*, Goldman v. Weinberger, 475 U.S. 503, 507 (1986) ("when evaluating whether military needs justify a particular restriction…courts must give great deference to the professional judgment of military authorities . . .").

[135] *See, e.g.*, United States v. Carr, 25 F. Cas. 306, 308 (S.D. Ga. 1872). Though neither can the service member who issued the order escape liability by claiming that he did not commit the unlawful act. *Id.*

[136] Note that ignorance of the law is no more a defense in military law than it is in civil law. In fact, even ignorance of a lawful general order is no defense, so without notice a service member might find herself subject to—and in violation of—a general order. *See* MCM, *supra* note 96, at II-114, ¶ R.C.M. 916(k)(3)(C)(1) ("(1) *Ignorance*

earlier, even experienced judges may have difficulty navigating the legal labyrinth to determine how an order aligns with the constellation of higher-order laws. And the deferential approach to military orders in civilian courts implies that, more often than not, a service member stricken by dread that an order is unlawful will rarely find a sympathetic audience in a courtroom.

Part of the problem is that soldiers should not be amateur jurists, questioning and wondering when they ought to obey and act.[137] Moreover, jurists should not be amateur (or armchair) commanders. This is the wide pass most military orders must march through—between the steep walls of a perceived need for absolute obedience within the military's ranks on one side, and the reluctance of judges to interfere in "'the customary military law' or 'general usage of the military service'" on the other.[138] This is not to say that these complementary principles are not reasonable, nor even that they are not essential. But there is reason for caution. As Justice Jackson noted in dissent in the now-infamous *Korematsu* case, "the Court . . . has no choice but to accept [a commander's] own unsworn, self-serving statement. . . . And thus it will always be when courts try to look into the reasonableness of a military order."[139]

Consider again the highly deferential standard articulated in *Huet-Vaughn*.[140] Even this standard is susceptible of the possibility

or mistake of law. Ignorance or mistake of law, including general orders or regulations, ordinarily is not a defense."). This raises the question of how a subordinate could possibly go through the above analysis to ascertain the legality of that order. *See id.* at R.C.M. 916(d). Fortunately, when a general order is unlawful, it tends to be of the sort that a service member's observation of its mandate will not cause her to incur liability.

[137] In the Navy, an enlisted sailor who is ever vigilant in asserting his rights (or advising others of their rights) and citing regulations in defiance of his supervisors is referred to as a "sea lawyer." It is not typically considered a compliment. *See* Steven F. Momano, *Wegmans Incident is Sign of a Bigger Problem in America*, DEMOCRAT & CHRON. (Apr. 25, 2015), http://www.democratand chronicle.com/story/opinion/guest-column/2015/04/25/wegmans-incident-sign-bigger-problem-america/26324715/.

[138] Parker v. Levy, 417 U.S. 733, 744 (1974) (quoting Martin v. Mott, 25 U.S. 19, 35 (1827)).

[139] Korematsu v. United States, 323 U.S. 214, 245 (1944) (Jackson, J., dissenting).

[140] United States v. Huet-Vaughn, 43 M.J. 105, 114-15 (C.A.A.F. 1995).

that a soldier might permissibly violate an order—even that there might be a "duty to disobey" such an order.[141] In practice, though, courts apply this standard in one of two ways, and neither encourages the view that courts will willingly explore the contours of that narrow forbidden zone. The first and most common way that courts have applied this standard is to punish disobedience of orders that were insufficiently unreasonable.[142] In fact, on review, courts tend to find orders not only reasonable enough not to be disobeyed, but lawful in their own right.[143] The same is typically true when service members challenge orders or regulations in court as unlawful, including when the challenge is for unconstitutional vagueness[144] or for violating a constitutionally protected privilege.[145] Leaning heavily on the twin pillars of order and discipline, Justice Stewart wrote in *Greer v. Spock* that "a military commander [can act] to avert what he perceives to be a clear danger to the loyalty, discipline, or morale of [those] under his command," even when such action chafes against constitutionally protected liberties.[146] For instance, this was all the

[141] *Id.*

[142] *See*, *e.g.*, United States v. New, 55 M.J. 95, 107-08 (C.A.A.F. 2001) (upholding conviction against service member for failing to wear United Nations accoutrements in Macedonia despite personal belief in the illegality of the order to don those accoutrements).

[143] *Id.* at 107.

[144] *See, e.g.*, Parker v. Levy, 417 U.S. 733, 756-57 (1974) (holding UCMJ articles authorizing court-martial for charges arising under Articles 133 and 134 not unconstitutionally vague). This case is also apposite in that the Court addresses the uncertainty inhering in these vague—though not unconstitutionally so—articles. Justice Rehnquist explains that "even though sizable areas of uncertainty as to the coverage of the articles may remain after their official interpretation by authoritative military sources, further content may be supplied even in these areas by less formalized custom and usage." *Id.* at 754 (citing Dynes v. Hoover, 16 U.S. 65, 82 (1857)).

[145] Brown v. Glines, 444 U.S. 348, 358 (1980) (finding constitutional a regulation requiring prior approval from commanders to circulate petitions, and holding that regulation did not violate federal statute stating that no person may restrict any service member from otherwise lawfully communicating with a member of Congress). *See generally* Nicole E. Jaeger, *Maybe Soldiers Have Rights After All! Loving v. United States, 116 S. Ct. 1737 (1996)*, 87 J. CRIM. L. & CRIMINOLOGY 895 (1997) (describing the development of the Supreme Court's standard of review for service member claims of constitutional violations).

[146] Greer v. Spock, 424 U.S. 828, 840 (1976) (holding that military regulations forbidding partisan political speeches and demonstrations and distribution of

specificity needed to justify a prohibition against circulating political literature on base.[147]

The other circumstance in which a court might apply the "no rational doubt" standard of *Huet-Vaughn* is when such an order was plainly issued and then followed. Convictions in American courts for war crimes are notoriously difficult to obtain. Following the My Lai massacre, only one soldier, the officer in charge, was convicted despite his having had numerous enlisted soldiers under his command. His life sentence was later reduced to a short term of years under house arrest.[148] More recently, Marines who were convicted or had reached plea deals relating to their roles in atrocities committed in Hamdania, Iraq, either had their convictions reversed or received clemency reducing their sentences.[149] The aftermath of the massacre at Haditha, Iraq, paints a similar picture of prosecutorial and judicial impotence to assign responsibility to soldiers near the field of battle.[150] Thus, one is left with the distinct impression that a soldier's perceived risk of obedience, even to an order providing "no rational doubt" of its illegality, is outweighed by the perceived risk arising from a failure to obey.[151]

---

political literature without approval from post headquarters was not a violation of the First and Fifth Amendments).

[147] *Id.* at 107.

[148] KENDRICK OLIVER, THE MY LAI MASSACRE IN AMERICAN HISTORY AND MEMORY 232 (Manchester Univ. Press 2006).

[149] Teri Figueroa, *General Frees Another Marine Convicted of War Crimes*, NORTH CTY. TIMES (Aug. 11, 2007), http://www.nctimes.com/news/local/general-frees-another-marine-convicted-of-war-crimes/article_b68ce24a-c3c7-5a3c-8ba3-633ed9f334a0.html; Teri Figueroa, *No Jail for Corporal in Hamdania Killing*, NORTH CTY. TIMES (Aug. 3, 2007), http://www.nctimes.com/news/local/article_ 1a92df09-ebda-5ea3-9253-883b77864a98.html; Mark Walker, *Military: Court Throws out Hamdania Conviction*, NORTH CTY. TIMES (Apr. 22, 2010), http://www.nctimes.com/news/local/military/article_5c4f1616-8c6e-5c0d-9500-3e63464e695b.html.

[150] Tony Perry, *Court-Martial to Begin for Marine in Iraqi Killings*, L.A. TIMES (Jan. 6, 2012), http://www.latimes.com/news/local/la-me-court-martial-20120106,0,4957742.story.

[151] Perhaps this stark choice serves at least to reduce some of the effective uncertainty in the process by constraining outcomes (or at least perceived outcomes) within the context of courts-martial.

Simply put, low-ranking military service members in the heat of combat are expected to make complex evaluations regarding the legality of the orders they are given and expected to obey or face the consequences. To further complicate matters, the potential consequences for failure to obey are maximized, and the practical consequences for obeying even plainly illegal orders are almost negligible. This has the effect of making even egregiously errant battlefield orders more legitimate than general orders and regulations. "All orders, written or oral" Colonel Winthrop explained, "made or given by any competent authority, from the commander-in-chief to an acting corporal, are indeed in a general sense a part of the law military; their observance by inferiors being strictly enjoined and their non-observance made strictly punishable."[152] This is the ever-present admonition embedded in Lord Tennyson's observation: "Theirs not to make reply; theirs not to reason why; theirs but to do and die."[153]

As though in an afterthought, the end of Winthrop's chapter on military regulations and orders includes a single unnumbered, paragraph-long subsection entitled "Principles Governing Orders." Here Winthrop provides a lonely caveat to the obedient soldier.

> As in the making of Regulations, so in the framing of Orders, the principles heretofore laid down to the effect that executive acts may not trench upon the province of legislation, or conflict with the existing constitutional or statutory law, are to be strictly observed. Further, Orders should not conflict with established Regulations. And Orders issued by commanders of departments or armies, or other military authorities inferior

[152] WINTHROP, *supra* note 85, at 38. Note that "an acting corporal" holds the pay grade of E-4, which is the lowest noncommissioned officer rank. Some enlisted members hold this rank before reaching their first non-training command.
[153] Alfred Tennyson, *The Charge of the Light Brigade*, POEMS OF THE ENGLISH RACE 119 (Raymond M. Alden ed., 1921). Though not Lord Tennyson's original wording (and corrected in all later printings), his wife's error in the poem's first printing was not inapposite: "theirs but to do *or* die" (emphasis added). CHRISTOPHER B. RICKS, TENNYSON 359 (2d ed. 1989).

> to the President, may not contravene the orders of the latter as Commander-in-Chief.[154]

In short, orders must be consonant with the Constitution, statutes, and regulations, as well as superior orders—all bodies of law that might not be familiar to a newly minted private. But if the order conforms, it is to be unquestioningly obeyed. The obvious problem is in getting from unquestioning obedience of orders to thoughtful discernment of an order's legal virtue.

That problem of moving from unquestioning obedience of orders to discerning the lawfulness of an order is the paradox of law at this most quantum end of the spectrum. Prospective assessment of an order's legality is a Gordian knot of overlapping law and, as a result, is a highly unpredictable process. But a semblance of certainty is restored because courts, when retrospectively examining the legality of an order *vel non*, are likely to cut the knot in favor of obedient subordinates. Society entrusts the power to issue orders to the commissioned officers, warrant officers, noncommissioned officers, and petty officers because these military personnel are in a much better position to judge what is necessary in a given situation and are more accustomed to making decisions of a variety most common to the military and most alien to civilians. Nonetheless, efforts to ensure that military personnel are more conscientious of the law necessarily have the side effect of deterring obedience (or at least of delaying it) because it places the burden of legal analysis onto the subordinate. Hence, there is a tradeoff between knowledge of the law and the surety of obedience. Just as the rules governing quantum phenomena in the physical world resist any effort to significantly reduce indeterminacy, so too does quantum lawmaking resist such efforts.

Not only does quantum lawmaking limit the predictability of an order's legality and of the potential consequences for obedience or disobedience, but its sheer chaos and strangeness also numb us to its implications. Just as quantum mechanics is irrelevant to a soldier on the field, society might forgive a soldier for asking who really cares

[154] WINTHROP, *supra* note 85, at 33.

whether a sergeant's order is more like quantum law or more like classical law. The foregoing discussion certainly suggests that military members gain no particular advantage in worrying over the direct consequences to themselves stemming from the strangeness of the law they are immersed in. But a discussion of consequential concerns portrays the soldier as only the grammatical object of our inquiry. The most important policy implications of quantum law on the battlefield, though, emanate from the soldier's preeminence in the quantum calculus. It is not unlike how an average person, never having heard of quantum mechanics, can go her whole life without thinking about it. But our modern life depends inescapably on quantum-mechanics-informed technology (to say nothing of the fact that our very existence is possible because of quantum phenomena). One can ignore the very small, but it does not go away. And it is probably important to us even if we do not know it.

III. HOW POLICY GETS TIED DOWN BY LILLIPUTIAN LAW

Our soldiers, sailors, and Marines are, as the saying goes, the "tip of the spear." But this description's instrumental flavor fails to reflect an important facet of the military's function. At the disposal of our forward-deployed military is the not-insignificant power permeating the legal quanta of their profession. Order-issuing authority in the sensitive zone of engagement occupied by the military is not only an instrument of policy; it can also force policy on the military's civilian leadership and on the public at large. In fact, the legal constraints on authority in its ranks notwithstanding, the military's specialized and systematized nature makes the military a potent sensory organ of a state's policymaking apparatus. Information flows into and out of a state's decision-making process through its operational military, and no part of a state's government is so designed for action as its armed forces. And even as a thoroughly explored phenomenon in classically understood policymaking and decision making, this can be an unnerving fact to confront. The idea that a poorly understood legal uncertainty pervades our military evokes images of restless seismic activity rumbling hidden beneath the surface of our national security environment. Nevertheless, as described below, policy sometimes

makes its way from "the front" to a decision maker situated to the rear.

A. Policy Creation in Conflict – the Rational Actor Model

For thirteen excruciating days in October of 1962, the world was about to end.[155] Since then, volumes of history have been written about the Cuban missile crisis, mostly in the form of gripping narratives brimming with real-life, existential suspense. Nine years later, one author, though, went beyond the *story* of what happened; Graham Allison instead fashioned a *theory* of what happened in his influential book entitled Essence of Decision.[156] In doing so, Allison revolutionized how scholars think about decision making.

The primary target in Allison's sights was the rational actor model ("RAM") of decision making.[157] RAM describes the world of states, organizations, and individuals as unitary black boxes. Stimuli enter the box through whatever means are available, the mysterious internal clockwork conducts a cost–benefit analysis using the available data, and from the black box of the decision-making state, organization, or individual springs a decision carefully weighed to produce what the actor sees as an optimal result. Then the process begins anew. This analytical method is a powerful tool. By positing a world based on RAM, a clever analyst can reverse engineer every

[155] This was, of course, the Cuban missile crisis. The American discovery of Soviet missiles in Cuba precipitated a standoff between the two nuclear superpowers. President Kennedy instituted a blockade against Cuba to prevent further shipments of missiles from the U.S.S.R. At the same time, the Kennedy Administration sought a compromise through diplomatic back channels with Soviet Premier Khrushchev. Despite heated public rhetoric and the fear in Washington that a coup of hardliners had overthrown Khrushchev, the countries were able to negotiate a deal to remove the missiles from Cuba in exchange for a later, ostensibly unrelated removal of NATO missiles from Turkey. Equally important, the United States did not have to sacrifice NATO presence in West Berlin, which was likely the extraction the Kremlin truly sought with its Cuban gambit. *See generally* ROBERT F. KENNEDY & ARTHUR SCHLESINGER, THIRTEEN DAYS: A MEMOIR OF THE CUBAN MISSILE CRISIS 7-15 (1999).

[156] *See generally* GRAHAM ALLISON & PHILIP ZELIKOW, ESSENCE OF DECISION: EXPLAINING THE CUBAN MISSILE CRISIS (2d ed. 1999).

[157] Though his analysis targeted this theory as inadequate to the task of explaining away major political events, Allison himself is credited with coining the term RAM in ESSENCE OF DECISION itself. *Id.* at 3–4.

decision. The more bizarre or irrational an action seems, the cleverer the analyst must be, and success means erecting a bridge, however structurally tenuous, between the information available to the decision maker and the action finally decided upon. This was the good news preached by evangelical economists.[158] Political scientists, eager to apply their craft to the problem of understanding the interplay of power, principles, and agents, were eager converts. Thus, when Allison wrote Essence of Decision, RAM—by one name or another—was the prevailing orthodoxy. And it was this orthodoxy Allison's work expanded upon and, in many senses, displaced.

"Among the most remarkable features of current life," Allison wrote, "is how much behavior of how many individuals is influenced by the controlling purposes of the organizations to which they belong."[159] Thus Allison began to describe how the procedures that organizations create for themselves embody Weberian principles of organization. To be clear, creating procedures is a purposive activity. The heads of organizations see a goal and attempt to effect (or at least *affect*) policies to achieve the goal.[160] Allison was not saying that rationality is not a real phenomenon. Rather he was saying that rationality is but one aspect of the story.[161] More important, he was saying that what happens inside the black box is not just a complex equivalent to a set of scales on which decision makers weigh and divide costs and benefits. Multifarious factors affect what happens inside the black box, and the standard operating procedures (SOPs) that organizations adopt are a significant part of the machinery that interprets those factors. Quite often, Allison concluded, SOPs are themselves factors in this calculation.[162]

Allison's analysis, like the principles of quantum mechanics described above, cannot receive adequate justice here. But for this discussion, two aspects of Allison's view of what he called the Organizational Behavior Paradigm (OBP) of decision-making theory

[158] *Id.* at 19.
[159] *Id.* at 147.
[160] *Id.* at 148.
[161] *Id.* at 3.
[162] ALLISON & ZELIKOW, *supra* note 156, at 169.

are of particular value. First, it is important to understand that organizations like the military are no more monolithic than they are structureless. A military (like its subordinate units) is an organizational actor comprising many constituents and residing within a greater "constellation of loosely allied organizations on top of which government leaders sit."[163] An organization is a complex machine continuously abuzz with both autonomous and automated components. Action is the output of organizational machines, but organizational output is conceptually incompatible with RAM; no matter how we would like to look at an organization as an irreducible black box, its constituents, their actions, and their motives cannot be ignored.[164]

This conception of "action as organizational output"[165] is the other element essential for understanding the broader implications of quantum uncertainty in the military context. "The preeminent feature of organizational activity is its programmed character: the extent to which behavior in any particular case is an enactment of pre-established routines."[166] Allison identified seven characteristics of organizational activity: (1) objectives (where compliance with targets and constraints defines acceptable performance); [167] (2) sequential attention to objectives (whereby "conflicts among operational targets and constraints [are] resolved," [168] (3) SOPs (conventions for performing regular or coordinated activity that are "grounded in the . . . norms of the organization or the basic attitudes, professional culture, and operating style of its members"); [169] (4) programs and repertoires (formal "clusters" of rehearsed SOPs that are essential for performing an organization's special capacities);[170] (5) uncertainty avoidance (organizational efforts to "maximize autonomy and regularize the reactions of other actors

[163] *Id.* at 166.
[164] *See*, *e.g.*, *id.* at 307 ("The diverse demands on each player [in the organizational command structure] influence priorities, perceptions, and stands.").
[165] *Id.*
[166] *Id.* at 168.
[167] *Id.*
[168] ALLISON & ZELIKOW, *supra* note 156, at 169.
[169] *Id.*
[170] *Id.* at 170.

with whom they must deal");[171] (6) problem-directed search (organizational efforts to apply existing routines or capacities to novel or atypical problems for which those routines and capacities were not designed);[172] and (7) organizational learning and change (the process by which new problems are incorporated into regularized practices and procedures).[173] In other words, an organization makes procedures based on its culture and resources, assembles these SOPs into assorted programs for action, and attempts to apply those programs to problems. If the problem is unlike those the organization planned for, those programs that best fit the problem are deployed, and the new problem is then incorporated into the organization's procedures along with the lessons learned from applying those "close-enough" programs to it.[174]

What this had to do with the Cuban missile crisis (and what it has to do with the law of military orders, as well) is that military action is the product of the process described above. That holds true whether examining activities accompanying the clandestine installation of Soviet missiles less than one hundred miles from American shores, the failure to camouflage those missiles,[175] the practice of observing Cuba from U2 spy planes,[176] or the procedures for handling film taken of Cuba in those missions.[177] The cybernetic process by which organizations routinely operate and act literally makes history. Hence, the members of a military that form its operational tendrils are not only agents of their government, their military, and their unit, but are also the media through which those organizations respond to their environments. Despite the veneer of

---

[171] *Id.*
[172] *Id.* at 171.
[173] *Id.*
[174] *See* Herbert A. Simon, *Rational Choice and the Structure of the Environment*, 63 PSYCHOL. REV. 129, 129-30 (1956). This is a departure from RAM's search for "optimal" choices in favor of those that merely "satisfice." Satisficing is a decision-making theory term of art that refers specifically to how thinking entities (originally individual humans, but more commonly today referring to organizations) seek out *any* solution to a problem and opt for the first that will work. This formulation makes order in time, rather than optimality, the determinative consideration. *See id.*
[175] ALLISON & ZELIKOW, *supra* note 156, at 212-13.
[176] *Id.* at 219.
[177] *Id.* at 222.

rationality one might imagine over military decision making, some decisions are made by procedure alone, some are made because of the repertoire of procedures available, and some cannot be made were it not for the policies in place. This is the essence of the OBP, and it is an important analytical tool for understanding the complex of organizational actions that populate the national security operating environment (and, for that matter, the business, diplomatic, and political environments to which these principles also apply).[178]

But this article examines SOPs as Graham Allison did not. For him, an SOP is an SOP, whether aimed at selling one million Big Macs in a certain amount of time while keeping labor and food costs below a certain level, or at monitoring a tiny neighboring island for signs of potential danger while avoiding a nuclear holocaust. And this is a perfectly respectable way of thinking about organizational behavior itself. But the military SOP as described here is more than just a procedural duct by which organizational capacities flow more or less perfectly to organizational problems. With criminal penalties to back them, military SOPs are also a kind of law according to this article's working definition.

When viewed together, organizational decision-making theory and the delegation of lawmaking authority to all but the lowest echelons of the military suggest that these servicemen and women are doing something more than merely promulgating an odd kind of law. They are also making policy. A poor understanding of the mechanisms that underlie the authority they wield means something more than an inability to comprehend the potential for punitive consequences. It also means an inability to comprehend the power entrusted to what are essentially low-level organizational employees—armed bureaucrats.

[178] Though not particularly relevant to the subject of this article, note that RAM and OBP were not the only models covered by Allison. *See id.* at 255. He also enunciated a model he called the Governmental Politics Model, which places more emphasis on individuals within an overarching bureaucratic structure. *See id.* Thus, to the OBP model is added the wrinkle of autonomous political actors who head governmental organizations and who, therefore, have at their disposal the organizational capacities to serve their agendas.

B. Policy Making by Combatants—an Example

To illustrate this point, consider a hypothetical scenario wherein U.S. ground forces are patrolling a stretch of border between Afghanistan and Pakistan. Governing these soldiers' on-duty actions are a network of interrelated and overlapping laws. The Constitution prevents them from seizing, without due process, property from American humanitarian workers or journalists. The statutory framework of the UCMJ does not permit them to desert their posts and search for greener pastures in the tribal regions of Waziristan. Department of Defense ("DOD") regulations would define their rules of engagement ("ROE") such that they can use deadly force only if they confront imminent, life-threatening danger. Army regulations might dictate how they wear their distinctive combatant insignias. The General Orders of a Sentry require that they not leave their assigned posts until properly relieved.[179] Perhaps their commander directed that no patrol group may have fewer than three soldiers. Maybe their officer in charge needs them to return early to attend a briefing, and so she ordered them to rendezvous at their checkpoint thirty minutes earlier than scheduled.

Every step in the chain above has legal force as to these soldiers. That a violation of any of these orders might invite legal consequences is unquestionable. Taking the scenario a step further, suppose the patrol comprises five soldiers: one sergeant, two specialists, and two privates. The group takes fire, which triggers their ROE. Their attackers stop firing and run for a small border village nearby. If these soldiers comply with all the laws described above,[180] the gamut of permissible actions is broad. The soldiers might pursue the attacker, they might call for reinforcements, or they

---

[179] *See, e.g.*, THOMAS J. CUTLER, THE BLUEJACKET'S MANUAL 153 (Naval Inst. Press 2002).

[180] The exception, perhaps, is the order to return early. It is hard to imagine that a commander would charge a subordinate soldier with—let alone get a conviction for—absence without leave or failure to report in the event that the subordinate had come under hostile enemy fire. *See generally* ALLISON & ZELIKOW, *supra* note 156, at 154-57.

might return to base to report the incident.[181] But whatever happens next, what the sergeant says to the four junior-enlisted personnel will be law. Considering only their first option, alarming potentialities spring to mind. Following attackers into a village means possible civilian casualties. It also spells the possibilities of house-by-house searches, booby traps, ambushes, and a civilian population sympathetic to the attackers. If the village were in Pakistan instead of Afghanistan, conflict between the United States and Pakistan might be implicated.

In short, the decisions made by our hypothetical unit of five soldiers have suddenly become a catalyst for national policy. The civilian leadership in Washington will be bound to respond to the hand dealt them by a single noncommissioned officer and the lawful orders he issued to his subordinates. The more discretion that sergeant has, the more difficult it is to predict the outcomes of his action, the legal effects on him and his subordinates, and the extent to which the organizations to which he belongs—all the way up to the federal government—will have to respond to restore a policy in equilibrium.

We should not heap all the blame on our hypothetical sergeant, though. He is partly the victim of policies that failed to see far enough ahead. Further, he was responding to an enemy, with the legal force entrusted to him by his lawful superiors. Thus, not only has our sergeant entangled us in an "international incident," but so for that matter have our enemies. Parties whose interests are diametrically opposed to those of the soldiers' nation had a hand in devising a situation that has led to a diplomatic crisis with our allies in Pakistan, who are already ill at ease with the proximity and character of our "support."[182] In essence, the action associated with quantum law on the battlefield turns the usual relationship between law and policy on its head. Whereas some assume that law follows

[181] Of course, their course might be dictated by preexisting SOPs, but this serves at least as an illustration of what might happen when reality progresses beyond the scope of the SOP. *See generally id.* at 154-57.

[182] *See* Joshua Foust, *U.S. Drones Make Peace With Pakistan Less Likely*, THE ATLANTIC (July 12, 2012), http://www.theatlantic.com/international/archive/2012/07/us-drones-make-peace-with-pakistan-less-likely/259756/.

from policy, this model suggests that sometimes policy follows from the action of law.

This represents a fundamental problem in any theory that proposes to justify the legal force of military orders. The philosophical underpinnings of "law" as used in this article require a societal basis. I have largely skirted this criterion by referring to law affecting only "military society" or by invoking our civil society's acquiescence to the manner in which the military is organized. One might even note that in a democracy defended by an all-volunteer force, the divide between the military and civilian societies is semipermeable. Yet these arguments are eroded by the revelation that our enemies may have as much to say about some of our law as our citizens do. Obviously, laws and policies shaped in part—even if unconsciously—by actors bent on our annihilation might not reflect our societal values all that well.

Once one accepts the possibility that poorly reflected societal values in military law matter, other examples, lurking furtively in the wings, subtly insinuate themselves into the analysis. Military orders are a form of public law. But as compared to other bodies of public law in the United States, military orders are antidemocratic. To fully appreciate this democratic deficiency, one needs only to consider the uniformity of military orders from one society to the next. Orders issued in the Chinese military are similar in purpose and kind to those of the Russian military, those of the Dutch military, those of the Cuban military, and those of our own. What those orders authorize does not vary significantly among national militaries, regardless of whether that military serves a democratic state or an authoritarian one. It is often noted that our military's mission is to defend democracy, not to be one.[183] And as Justice Rehnquist put it, "military society has been a society apart from civilian society, so '(m)ilitary law . . . is a jurisprudence which exists separate and apart

[183] During my ten-year enlistment I heard this phrase more often than I can readily tally, and from a variety of authority figures. *See also* Deborah Grays, *Army to Celebrate 234 of 'Service Commitment'*, U.S. ARMY, June 5, 2009, http://www.army.mil/article/22210/army-to-celebrate-234-years-of-service-commitment/ (explaining that the U.S. army has worked to "guarantee freedom, preserve peace and defend democracy" since 1775).

from [civilian law].'"[184] That this unpredictable subset of law is so *proudly* antidemocratic is a provocative fact, and it suggests a tension not wholly unrelated to that more notorious tension prevailing between the values of democracy and the so-called military-industrial complex.[185]

Unpredictability itself may be an unseemly feature for any form of law to embrace. Although unpredictability besets all laws—whether in terms of unforeseen consequences or of a law's efficacy before its implementation—laws are intended essentially to reduce uncertainty. After all, one of the basic justifications for issuing law in a systematic way and publicizing it is to provide our society with the benefits conferred by a predictable regime and well-founded expectations on which to rely. Even military law, according to Graham Allison, is constructed to reduce uncertainty.[186] But by embracing as law activity that thrives in and propagates uncertainty in the military context, society defiantly rejects the logical desire for predictability that motivates nearly all other forms of law.

Other forms of law in the United States must meet certain procedural standards, and in this regard, military law is theoretically no different. But because evaluating the validity of orders is an endeavor steeped in uncertainty, courts may be ill equipped to review them. Indeed, it is to a lack of expertise that judges often adduce when demurring to intervene in matters involving a commander's discretion to regulate subordinates.[187] Even before judicial review

[184] Parker v. Levy, 47 U.S. 733, 744 (1974) (quoting Burns v. Wilson, 346 U.S. 137, 138 (1953)) (alteration in original).

[185] President Dwight D. Eisenhower, Farewell Address to the Nation (Jan. 17, 1961) ("[t]his conjunction of an immense military establishment and a large arms industry is new in the American experience. The total influence—economic, political, even spiritual—is felt in every city, every Statehouse, every office of the Federal government. We recognize the imperative need for this development. Yet we must not fail to comprehend its grave implications. Our toil, resources and livelihood are all involved; so is the very structure of our society.").

[186] ALLISON & ZELIKOW, *supra* note 156, at 170.

[187] *See, e.g.*, Goldman v. Weinberger, 475 U.S. 503, 507 (1986). In cases involving peculiarly military offenses, like that of Article 134, perhaps this reluctance is akin to the analysis pertaining to the APA's exemption of judicial review for "agency action…committed to agency discretion by law." Application; Definitions, 5 U.S.C. § 701 (1978). The judicial gloss on this portion of the APA has evolved so as to be

becomes a possibility, process in this context is minimal compared with other instances of law and lawmaking. As discussed above, a subordinate has almost no opportunity when given an order to consider its validity or potential consequences. And because issuing orders is itself lawmaking, it is a form of prescription untethered from process. This represents a significant practical difference between "normal" rulemaking and prescription in the military context. Consider the difference between a regulation held to be an acceptable interpretation of a statute but arrived at arbitrarily or capriciously,[188] and an order that seems legal in every way but that is *in fact* arbitrary or capricious.[189] The former will be struck down; the latter must be obeyed.

To summarize, the United States military has a body of law and a method of lawmaking that, when viewed together, are bizarre (even foreign) to our system of justice and jurisprudence, but that are nonetheless fundamental to the fabric of our republic. This law—and I hope I have sufficiently established that it *is* law—is antidemocratic, nearly devoid of meaningful process, [190]

largely coterminous with the doctrine of "no law to apply," which was first enunciated in *Citizens to Pres. Overton Park, Inc. v. Volpe.* Citizens to Pres. Overton Park, Inc. v. Volpe, 401 U.S. 402, 410 (1971). But civilian courts make up only part of the story. Though it may be implicitly evident, it should be understood that most active-duty service members are not tried in civilian courts for military related offenses, but rather by military officers presiding over courts-martial. *See* MCM, *supra* note 96, at II-10, R.C.M. 201(d). Thus, even setting aside the issue of diffidence in civilian judges, important institutional biases may well inhere in the process. Courts-martial are not kangaroo courts; the procedural rights of defendants in courts-martial, in fact, can be so rigidly applied as to seem bizarre to the uninitiated. For instance, an accused service member who pleads guilty is subjected to an inquiry of the facts to ensure the plea is honest. *See id.* at II-100, R.C.M. 910. Nevertheless, the way in which military officers arrive at verdicts cannot help but be shaped by the military culture in which a court-martial's more regular participants are immersed.

[188] *See, e.g.*, Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 30 (1983).

[189] This assertion follows naturally from the highly deferential *Vaugh-Huet* standard, by which only "manifestly unlawful" orders may be lawfully disobeyed. United States v. Huet-Vaughn, 43 M.J. 105, 114-15 (C.A.A.F. 1995).

[190] This refers only to the lawmaking embedded within lawful orders. The adjudicatory branch of military law embodied by courts-martial provides ample

unpredictable, and partly forced on us by those against whom it is designed to protect. More troubling still, this law is the software for a military that functions as a tactile organ of national policy. Just as humans use their hands to learn about the world around them and to impose their will on that world, a military conveys information to its government and is called on to carry out the policy formulated in response to this information. The special role of the military and the organizational culture that role engenders shape how data arrive (and sometimes which data arrive). Information from "the front" thus carries with it a faint scent of the military's organizational biases. Though Justice Brewer perhaps did not have these facts and this metaphor in mind, they certainly complement his view of the military as "the executive arm."[191]

Just as the easily ignored scintillae of the quantum world can, despite our inattention, produce profound effects on the world around us, the tiniest quanta of military activity can change the course of nations and history. This activity is governed by a body of military law that spans from everyday regulation to the seething particulate chaos of battlefield orders. This latter category exemplifies quantum lawmaking. Although quantum lawmaking is typically hidden from sight, its effects on our society and our national policies can be profound. One cannot begin to understand those effects without understanding the causes that give them rise.

IV. CONCLUSION

In sum, quantum lawmaking is as important as it is strange. Its essence abides in all law, but we typically fail to perceive it, just as we fail to perceive the chaotic universe of the infinitesimal that abides in all the physical things whose predictability and stability we take for granted. This phenomenon superficially resembles in many regards the manner in which the smallest constituents of matter behave. Like quantum particles, quantum laws are unstable and contain unknown qualities until a judicial observation occurs and affirms their validity or snaps them back into the legislative ether.

procedure, and this should not be interpreted in any way as derogating that procedure. *See*, *e.g.*, MCM, *supra* note 96, at pt. IV-23, ¶ 16.c.(1)(a).

[191] United States v. Grimley, 137 U.S. 147, 153 (1890).

Before an observation, these "virtual laws" interact in various ways with one another and with other, already-observed laws in a way reminiscent of how unobserved quantum particles interact and interfere in the absence of observation. The vicissitudes of quantum lawmaking affect higher-order laws in ways that the legal community has come to expect, and so the strangeness seems mundane. But, as this article details, quantum lawmaking is not distributed uniformly across the varieties of legally binding norms.

The effects of quantum lawmaking amplify as laws descend further from the most general and stable legal norms of constitutional law. Thus, statutes are more quantum in character—and less classical—than constitutional law, and the level of instability increases down through federal regulation and various levels of state laws. Quantum lawmaking is increasingly difficult to ignore in the context of the law's narrowest and most specialized extremes, such as the contexts of private contracts and property transactions. But nowhere are these effects more pronounced than in the domain of national security law, and especially such laws as govern and pervade the armed forces. Military law is both extreme in its quantum character and powerful in its effect. Because an order formulated in an instant on the field of battle is inherently keyed to engage the criminal-legal apparatus if disobeyed, even the least formal breeds of military law can sometimes more closely resemble the force and generality of statutory law. Nevertheless, such orders still theoretically represent the least stable (that is, most quantum) legal norms in our system. The oddities that crowd around that extremity are compounded by how little society at large knows about military law and by the profound policy implications of such uncertainty in a context that so strongly affects national security and foreign policy.

These implications to national security and foreign policy are particularly profound given the invisible interactions and feedback effects that arise in large organizations. Studies of governmental organizational behavior in the national security environment reveal how efficiency-driven contrivances such as SOPs shape policy even as they are shaped by it. Military SOPs, however, unlike (for instance) most civil-service bureaucratic SOPs, are backed by force in a way that goes beyond simple policy or procedure and that instead

fit within this article's working definition of law. Military orders, including SOPs, are therefore an example of how legally binding norms can create channels that guide policy in ways that policymakers do not perceive. Moreover, because the military is responsive in some respects to hostile agents, one must conclude that "the enemy" potentially influences policy in similarly unseen ways.

Our collective reluctance to recognize this kind of activity as law further frustrates our ability to understand the implications of quantum lawmaking when we encounter it. When confronted with a legal phenomenon that frays the veil over this hidden quantum essence, courts and legal scholars equivocate. They declare that such a phenomenon is not law at all (and even that its quantum character makes the notion of its legal force "simply self-refuting"). Or they explain that it is only law in some abstract or hypothetical sense. They avert their eyes. This article proposes that the judiciary and the legal academy face this oddity head-on. In examining this extremity of quantum lawmaking, we as a society might ultimately decide that the practical necessities of the military's special responsibilities to the country, or that the military's highly insulated position within the executive in fulfilling the most executive of functions, justify this vertiginous heterodoxy. Indeed, these arguments might justify them fully. But by glossing over the most bizarre attributes of quantum lawmaking, especially in the context of national security law, we systematically fail to understand this narrowest scope of military activity for what it is. It is law, and law with important national security policy implications, at that. It may lack the doctrinal neatness of some areas of law—although those other areas perhaps have a beauty that is only skin deep. But it is law nonetheless. It emanates, albeit distantly, from the same constitutional fabric from which our other laws are fashioned. And it affects society in important ways, whether we see it or not.

COMMENT

TERROR IN MEXICO:
WHY DESIGNATING MEXICAN CARTELS AS TERRORIST ORGANIZATIONS EASES PROSECUTION OF DRUG TRAFFICKERS UNDER THE NARCOTERRORISM STATUTE

Stephen Roy Jackson*

In 2006, Felipe Calderón assumed the Mexican presidency and triggered one of the bloodiest drug wars in modern history. With deaths numbering in the tens of thousands, this threat continues to impact the United States today. The emergence of Los Zetas and the Vicente Carrillo Fuentes Organization led to a new form of terrorism garnering recognition by the United States. Congress acted against this threat by passing a law widely recognized as the "Narcoterrorism Statute," which increases mandatory minimum sentences for anyone found guilty of aiding a terrorist group through illicit drug cultivation or sales. While Congress previously failed to pass legislation officially recognizing Mexican drug cartels as foreign terrorist organizations, this idea should be revisited in order to implement an aggressive extradition campaign to the United States to prosecute members of these cartels for violating the Narcoterrorism Statute. This campaign would help counter the reign of terror brought by these cartels on both Mexicans and Americans alike.

* Candidate for J.D., George Mason University School of Law, May 2016. I want to thank Lauren Doney for her advice and guidance through the drafting process. I would also like to thank Donna Jackson for all of her advice and support.

INTRODUCTION

On a barren road in the hot desert, a decapitated body lies next to an idling car. A masked man appears from behind the vehicle and opens fire on a group of local farmers as they pass by. Several are killed and dumped in a mass grave adjacent to the road. While this scene may conjure images of war torn Afghanistan or Syria, it is in fact a portrayal of narcoterrorism commonly found in Mexico.[1]

[1] *See* Daniel Tovrov, *Mexico Drug Wars: Zetas Cartel Boss Reveals Mass Graves*, INT'L BUS. TIMES (Feb. 9, 2012), http://www.ibtimes.com/mexico-drug-war-zetas-cartel-boss-reveals-mass-graves-408216; Randal C. Archibold, Editorial, *Drug Kingpin Is Captured in Mexico Near Border*, N.Y. TIMES (July 15, 2013), http://www.nytimes.com/2013/07/16/world/americas/drug-kingpin-is-captured-in-mexico-near-border.html?_r=0 (explaining that Los Zetas is known for decapitating and

Since Felipe Calderón assumed the Mexican presidency in 2006, drug-related violence has risen to an unprecedented level. This cartel [2] violence has affected more than 100,000 Mexican households, caused more than 20,000 disappearances, and resulted in at least 90,000 deaths.[3] The poorly controlled southern U.S. border has only exacerbated matters. Insufficient border enforcement has allowed the Mexican drug war to traverse state lines, resulting in a reign of terror encompassing several American cities like El Paso and Phoenix.[4] Efforts to curtail cartel power in both Mexico and the United States have produced limited results.

Mexican drug cartels continue to pose a dangerous threat to U.S. citizens and national security. Responding to the militarization of these organizations, the U.S. government developed several programs to provide critical assistance to the Mexican government. These programs, like the Mérida Initiative, provide training to Mexican police forces, supply weapons and military equipment (such as Black Hawk helicopters), and increase financial assistance to

dismembering its victims); Eduardo Castillo, *Mexico Migrants Massacre: Drug Cartel Suspected In Killing of 72*, THE WORLD POST (Oct. 26, 2010), http://www.huffingtonpost.com/2010/08/26/mexico-migrants_massacre_n_695299.html (explaining how drug cartels engage in indiscriminate murders).

[2] "Cartel" is defined as "[a] combination of producers or sellers that join together to control a product's production or price." BLACK'S LAW DICTIONARY (10th ed. 2014). Organizations in Mexico involved in the drug trade, irrespective of whether they continue to collaborate with other producers and sellers, are known as "Mexican drug cartels".

[3] *See* Marguerite Cawley, *Mexico Victims' Survey Highlights Under-Reporting of Crime*, INSIGHT CRIME, Oct. 1, 2014, http://www.insightcrime.org/news-briefs/6062-mexico-victimization-survey-highlights-reporting-gap; *Mexico Captures Gulf Cartel Leader Behind Wave of Violence*, NBC News, May 26, 2014, http://www.nbc news.com/news/world/mexico-captures-gulf-cartel-leader-behind-wave-violence-n114436; Evelyn Krache Morris, *Think Again: Mexican Drug Cartels: They Aren't Just About Mexico or Drugs Anymore*, FOREIGN POLICY, Dec. 4, 2013, http://www.foreign policy.com/ articles/2013/12/03/think_ again_mexican_drug_cartels.

[4] *See, e.g.*, Nina Golgowski, *Mexican Cartel Violence Spills into U.S. as 'Drug Assassin' Pleads No Contest to Beheading Man in Arizona*, DAILYMAIL.COM, March 7, 2013, http://www.dailymail.co.uk/news/ article-2289976/Arizona-beheading-Mexican-cartel-violence-spills-U-S-drug-assassin-pleads-contest-murder.html.

combat cartel violence.[5] Despite this assistance, the violence resulting from drug trafficking has not ceased.

In order to protect its border, its citizens, and its national security, the United States must identify a new solution to address the threat of cartel violence. The Controlled Substances Act of 2006 holds one possible solution. In section 960a of the Act,[6] Congress broadened the federal government's jurisdiction over offenders of U.S. drug and terrorism laws.[7] This statutory provision increases mandatory minimum prison sentences[8] for offenders who assist terrorist organizations via drug trafficking and cultivation.[9] There is no question that Mexican drug cartels violate U.S. drug laws, as they engage in drug trafficking, manufacturing, and cultivation.[10]

Given their propensity toward violence and politically based attacks, cartels pose a significant threat to American national security, and arguably constitute terrorist organizations. If the United States designated these groups as terrorist organizations, the Department of Justice ("DOJ") could apply section 960a jurisdiction to individuals assisting the cartels in the illegal narcotics market. This jurisdiction

[5] One of these programs, the Mérida Initiative, included training about 4,500 Mexican federal police, supplying $1.6 billion in funds, and offering technical assistance between 2008 and 2011. William Dean, et al., *The War on Mexican Cartels: Options for U.S. and Mexican Policy-Makers*, INST. OF POL. 31 (Sept. 2012), http://www.iop.harvard.edu/sites/default/files_new/research-policy-papers/TheWarOnMexican Cartels_0.pdf.

[6] Foreign Terrorist Organizations, Terrorist Persons and Groups, 21 U.S.C. § 960a (2006).

[7] *See, e.g.*, 151 CONG. REC. S9835, S9846 (daily ed. Sept. 8, 2005) (statement of Sen. Cornyn); 151 CONG. REC. H6273, H6292 (daily ed. July 21, 2005) (statement of Rep. Hyde).

[8] The recent Supreme Court decision of *Johnson v. United States* does change the process in which mandatory minimum sentences are implemented in the Armed Career Criminal Act. The broader implications of *Johnson* remain to be seen outside of the context of the Act. *See* Johnson v. United States, 135 S. Ct. 2551, 2553, 2574-75 (2015).

[9] *See* Foreign Terrorist Organizations, Terrorist Persons and Groups, 21 U.S.C. § 960a (2006).

[10] *See, e.g.*, Tristan Reed, *Mexico's Drug War: A New Way to Think About Mexican Organized Crime*, FORBES, Jan. 15, 2015, http://www.forbes.com/sites/strat for/2015/01/15/mexicos-drug-war-a-new-way-to-think-about-mexican-organized-crime/.

would authorize the government to take the necessary actions to combat cartel violence. Such designation would empower the government to increase captured cartel members' prison sentences. Applying this designation to Mexican cartels like Los Zetas and the Vicente Carrillo Fuentes Organization would ease extradition of their members and affiliates to the United States, which would better protect the nation's borders from this deadly threat. Imprisoning cartel members in the United States as terrorists would reduce the likelihood that these members would escape and reengage in narcoterrorism. It would also demonstrate that the United States has prioritized the prosecution of drug cartels and serve as a means of deterring prospective members from violating U.S. law.

This Comment explores the grave situation along the U.S.-Mexico border and the threat it poses to U.S. national security.[11] The United States must take a new approach to address this threat by invoking the "terrorist organization" designation under section 219 of the Immigration and Nationality Act, and prosecute cartel members and affiliates under section 960a of the Controlled Substances Act. A vital aspect of this new approach includes a paradigm shift within the Foreign Terrorist Organization ("FTO") classification system implemented by the Department of State. This Comment argues that those organizations that engage in both terrorist activities and political violence must be considered terrorist groups, regardless of whether they are also motivated by financial gain.

Part I of this Comment provides an overview of the current conflict in Mexico. This section details the terror wrought by the cartels and how this currently threatens both Mexico and the United States. This section identifies and examines four major drug cartels and determines that two should be considered FTO designation by the Department of State, while the remaining two operate as traditional

[11] Cartel members have engaged in assassinations and torture in the states of Oregon, Virginia, Minnesota, and South Carolina. While those killed tend to be cartel members themselves, this violence occurred in U.S. territory and may result in future American casualties. *See* Andrew O'Reilly, *Mexican Drug Cartel Violence Spreading To Rural U.S. As Police Crack Down In Big Cities*, FOX NEWS LATINO, Aug. 12, 2014, http://latino.foxnews.com/latino/news/2014/08/12/mexican-drug-cartel-violence-spreading-to-rural-us-as-police-crackdown-in-major/.

organized crime syndicates and should not be considered for FTO designation. These four cartels demonstrate that two types of Mexican cartels operate in Mexico: those that still operate as traditional organized crime and those that are terrorist organizations.

Part II details the definitions of "terrorist organization" and "terrorist activity" germane to section 960a and section 219.[12] After notifying members of Congress, the Secretary of State may add a foreign group to the FTO list under section 219.[13] The process of assigning an organization to the State Department's terrorist list is examined in conjunction with the application of section 960a jurisdiction to organizations or individuals.[14] This section also discusses the benefits of designating a group as a terrorist organization for the purposes of U.S. government extradition, prosecution, and sentencing.

Part III illustrates how the both FTO designation and section 960a jurisdiction are applied to an actual terrorist organization using the Fuerzas Armadas Revolucionarias de Colombia ("FARC") as a case study.[15] Specifically, this case study demonstrates how the FARC's designation as a terrorist organization led to the extradition of José María Corredor-Ibague to the United States for violating section 960a.[16]

Part IV addresses whether Mexican drug cartels meet the "politically motivated" element required for terrorist organization designation.[17] In particular, various actions, comments, and behaviors

[12] Designation of Foreign Terrorist Organizations, 8 U.S.C. § 1189 (2004). The Foreign Terrorist Organization label is paramount to the proposed extradition and prosecution scheme because of the persuasiveness of the label and its ability to unify all U.S. laws pertaining to terrorism.
[13] 8 U.S.C. § 1189(a)(2)(A)(i) (2004).
[14] 21 U.S.C. § 960a(b) (2006).
[15] English translation: the Revolutionary Armed Forced of Colombia-People's Army. *See Foreign Terrorist Organizations*, DEP'T OF STATE: BUREAU OF COUNTERTERRORISM, http://www. state.gov/j/ct/rls/other/des/123085.htm (last visited Sept. 21, 2015).
[16] John E. Thomas, Jr., *Narco-Terrorism: Could the Legislative and Prosecutorial Responses Threaten Our Civil Liberties*, 66 WASH. & LEE L. REV. 1881, 1889 (2009).
[17] For the purposes of section 219 of the Immigration and Nationality Act, to engage in "terrorism," an organization must engage in "politically motivated violence…" Annual Country Reports on Terrorism, 22 U.S.C. § 2656f(d)(2) (2004).

of Mexican drug trafficking organizations ("DTOs") illustrate that several cartels are politically motivated. These cartels seek to overthrow the Mexican government and establish de facto narcorule. In the event that they achieve this goal, the United States faces an even greater threat as its southern neighbor battles violence, economic instability, and political upheaval.[18] Furthermore, these cartels are rumored to hold relationships with U.S.-designated terrorist organizations like Hezbollah,[19] demonstrating a threat to American security interests.

Part V reviews potential jurisdictional challenges associated with the use of section 960a for Mexican cartels. To properly extradite cartel members to the United States, issues pertaining to extraterritorial jurisdiction must be considered. The U.S.-Mexico Extradition Treaty of 1978 and common law notions of extraterritorial jurisdiction grant the U.S. government the ability to extradite cartel members for prosecution.

This Comment concludes by proposing that designating several Mexican cartels as terrorist organizations and subsequently extraditing them to the United States for violating section 960a is a beneficial policy for battling narcoterrorism. U.S. law enforcement

---

[18] *See* Brett O'Donnell & David H. Gray, *The Mexican Cartels: Not Just Criminals but Terrorists*, 3 GLOBAL SECURITY STUDIES, 29, 38 (2012) (stating that Mexican cartels are "actively seeking to weaken the state [of Mexico] to continue their operations").

[19] *See* Press Release, Treasury Targets Major Money Laundering Network Linked to Drug Trafficker Ayman Joumaa and a Key Hizballah Supporter in South America (June 27, 2012), http://www.treasury.gov/press-center/pressreleases/Pages/tg1624.aspx (explaining that Ayman Joumaa, a high-level money launderer and drug trafficker, maintained connections with both Hezbollah and Los Zetas); Joel Hernández, *Terrorism, Drug Trafficking, and the Globalization of Supply*, 7 PERSPECTIVES ON TERRORISM 41, 42 (2013) (explaining that Hezbollah sought to use Ayman Joumaa and the Lebanese Canadian Bank to conduct narcotrafficking with Los Zetas); Terence Rosenthal, *Los Zetas and Hezbollah, a Deadly Alliance of Terror and Vice*, CTR. FOR SECURITY POL'Y (July 10, 2013), https://www.centerforsecurity policy.org/2013/07/ 10/los-zetas-and-hezbollah-a-deadly-alliance-of-terror-and-vice/ (claiming that Los Zetas assists Hezbollah in forming communities for Lebanese and Syrian immigrants in Mexico, and that Los Zetas partners with Iran's Quds Force). *Cf.* U.S. Dep't of State: Bureau of Counterterrorism, Country Reports on Terrorism 2013, at 217 (2014) ("[t]here are no known international terrorist organizations operating in Mexico, and there is no evidence that any terrorist group has targeted U.S. citizens in Mexican territory.").

must engage in a strategic extradition effort aimed at destabilizing the cartels while protecting innocent Mexicans and Americans from retaliatory cartel violence.[20] This process best serves American interests because it utilizes U.S. law enforcement in countering cartel terrorism without committing large military resources to Mexico. The tactical approach to countering cartel violence remedies previous mistakes made in countries like Colombia and reestablishes a safer southern border for Americans.

I. SETTING THE SCENE IN MEXICO

A. The Current Situation: Death and Destruction

The Mexican war against drug trafficking escalated in 2006, when Felipe Calderón assumed the Mexican presidency and began directly targeting drug cartels, destroying the status quo held for decades.[21] Since this initial effort, deaths resulting from Mexican cartel violence increased dramatically.[22] This war poses a major concern for the United States because of its close proximity to the southern American border. Reports indicate that the Mexican states of Chihuahua, Nuevo León, and Tamaulipas, which lie along the U.S.-Mexico border, have endured some of the deadliest cartel violence since Mexico's drug war began in 2006.[23] This region is

[20] *See* Vanda Felbab-Brown, *Despite its Siren Song, High-Value Targeting Doesn't Fit All: Matching Interdiction Patterns to Specific Narcoterrorism and Organized Crime Contexts*, COUNTER NARCO-TERRORISM AND DRUG INTERDICTION CONF., Sept. 16-19, at 5-8 (outlining the failures of targeting high value targets in order to decapitate Medellín and Cali leadership in Colombia).

[21] *See, e.g.*, Craig A. Bloom, *Square Pegs and Round Holes: Mexico, Drugs, and International Law*, 34 HOUS. J. INT'L L. 345, 359 (2012).

[22] Total murders in Mexico rose exponentially from 8,867 in 2007 to 27,199 in 2011 which was the largest increase in murders in the Western Hemisphere in two decades. *See* KIMBERLY HEINLE, ET AL., DRUG VIOLENCE IN MEXICO: DATA AND ANALYSIS THROUGH 2014 4 (Justice in Mex., ed., 2015). In 2014, the number of intentional homicides in Mexico was an estimated 15,649, which is a 13.8 percent drop from 2013. *Id.* at 7.

[23] In 2011, these states ranked in the top five deadliest states in Mexico. The state of Sinaloa, which is connected to the southern border of Chihuahua, was the third deadliest state that year, *See* JUNE S. BEITTEL, CONG. RESEARCH SERV., R41576, MEXICO'S DRUG TRAFFICKING ORGANIZATIONS: SOURCE AND SCOPE OF THE VIOLENCE 30 (2013).

predominantly controlled by DTOs and serves as direct transportation routes for drug smuggling into the United States.[24] Cartel members penetrate the border through these states and enter U.S. cities to distribute illegal substances on the streets.[25]

While there is no evidence to suggest that cartel members consistently target American citizens within the United States, they have not hesitated to murder Americans within Mexican territory.[26] According to the State Department, 81 Americans were murdered in Mexico in 2013, while 100 Americans were murdered in Mexico in 2014.[27] To put these statistics in perspective, in 2014, 55 American soldiers were killed in Afghanistan, and 127 were killed in 2013.[28] The fact that murder rates in Mexico are even remotely comparable to American military casualties in a declared war zone is serious cause for alarm.

B. Meet the Cartels: Four Major Players in Mexican Drug Trafficking

Although the number of DTOs currently operating in Mexico fluctuates, it is common to classify Mexican drug traffickers into nine main cartels.[29] Operations conducted by DTOs in Mexico tend to be

---

[24] *See generally* Eric Goldschein, *Following the Cocaine Trail: How the White Powder Gets into American Hands*, BUS. INSIDER, Dec. 8, 2011, http://www.businessinsider.com/cocaine-facts-2011-12?op=1 (including a map of drug smuggling routes entering the U.S. utilized by cartels).

[25] *See, e.g.*, JUNE S. BEITTEL, CONG. RESEARCH SERV., R41576, MEXICO'S DRUG TRAFFICKING ORGANIZATIONS 22 (2015) (noting that Mexican cartels operate in the U.S. as far north as Chicago).

[26] *See, e.g.*, Bob Ortega, *American Killed After U.S. Travel Warning in Nogales*, AZ CENTRAL, May 27, 2014, http://www.azcentral.com/story/news/arizona/2014/05/27/american-killed-nogales-travel-warning/ 9642615/ (reporting on an American killed execution-style).

[27] *Mexico Travel Warning*, U.S. DEP'T OF STATE, http://travel.state.gov/content/passports/english/alertswarnings/mexico-travel-warning.html (last updated May 5, 2015).

[28] IRAQ COALITION CASUALTY COUNT, icasualties.org (last visited Sept. 21, 2015).

[29] These cartels include the Sinaloa cartel, Los Zetas, the Gulf Cartel, Tijuana Cartel, Juárez Cartel, La Família, Knights Templar, Beltrán Levya Organization, and the Jalisco Cartel. *See* Malcolm Beith, *The Current State of Mexico's Many Drug Cartels*, INSIGHT CRIME, Sept. 25, 2013, http://www.insightcrime. org/news-analysis/the-current-state-of-mexicos-many-drug-cartels.

violent and pose a threat to enemy drug traffickers, government employees, police, and average citizens. This violence is a direct result of the ongoing turf wars fought between warring cartels and the Mexican government. While all of these DTOs employ tactics reminiscent of terrorism seen in nations like Afghanistan and Syria, many still operate like traditional organized crime syndicates.[30] The following sections examine four emblematic Mexican cartels that demonstrate the differences in tactics utilized by these various organizations. These descriptions will better define which Mexican cartels merit the terrorist organization designation and which do not.

1. The Sinaloa Cartel

Until 2011, the Sinaloa Cartel controlled more Mexican states than any other DTO.[31] Originating from a group of marijuana and poppy cultivators in the state of Sinaloa, this DTO grew into a dominant cartel, ultimately expanding its influence to reach 50 countries.[32] The organization previously employed current rivals like the Juárez Cartel and Beltrán Levya, but experienced a major fissure around 2008.[33] Joaquin "El Chapo" Guzman Loera ("El Chapo"), one of the richest and most wanted narcotraffickers in the world, headed the cartel until Mexican Marines and U.S. agents arrested him on February 22, 2014.[34] Though El Chapo escaped from a maximum-security prison in Mexico on July 11, 2015, the group's current leadership remains unclear.[35] Prior to El Chapo's escape, the Drug

[30] Traditional organized criminals, for instance Nicodemo "Little Nicky" Scarfo, gained reputations as ruthless murderers, but still functioned as mob bosses for the conducting organized crime. *See* PHILIP LEONETTI, ET AL., MAFIA PRINCE: INSIDE AMERICA'S MOST VIOLENT CRIME FAMILY AND THE BLOODY FALL OF LA COSA NOSTRA 11 (Running Press ed., 2012).

[31] Los Zetas surpassed Sinaloa Cartel in state holdings in 2011. *See* Kazi Stastna, *The Cartels Behind Mexico's Drug War*, CBC NEWS, Aug. 28, 2011, http://www.cbc.ca/news/world/the-cartels-behind-mexico-s-drug-war-1.1036931.

[32] *See* Kirk J. Durbin, *International Narco-Terrorism and Non-State Actors: The Drug Cartel Global Threat*, 4 GLOBAL SECURITY STUD. 16, 17 (2013); BEITTEL, *supra* note 25, at 14.

[33] The exact year of Sinaloa Cartel's division is disputed. *See* BEITTEL, *supra* note 25, at 15.

[34] *See* Stastna, *supra* note 31.

[35] *See* Jeremy Bender, *This will be 'El Chapo's' biggest challenge now that he's escaped from prison*, BUS. INSIDER, July 22, 2015, http://www.businessinsider.com/this-will-

Enforcement Agency ("DEA") extradited Jose Rodrigo Arechiga-Gamboa, a.k.a. "Chino Antrax," the supposed replacement for Guzman from the Netherlands.[36] While the Sinaloa Cartel's leadership void may alter the cartel's internal structure,[37] it will likely continue to function as a traditional organized crime syndicate. The cartel differs from its more violent contemporaries by relying primarily on bribery over violence.[38] Based on the more restrained manner in which the Sinaloa Cartel conducts business, it fails to engage in terrorist activities and must not receive terrorist organization designation.[39]

2. Los Zetas

Formed by members of Mexico's elite special forces unit, Grupos Aeromoviles de Fuerzas Especiales ("GAFE"), Los Zetas initially functioned as the Gulf Cartel's paramilitary arm until it became an independent DTO in 2009.[40] Los Zetas quickly developed a reputation for engaging in extreme violence and indiscriminately

---

be-el-chapos-biggest-challenge-now-that-hes-escaped-from-prison-2015-7 (suggesting that El Chapo may not automatically resume control of the Sinaloa Cartel).

[36] *Alleged Sinaloa Cartel Leader Extradited to the United States from the Netherlands*, DEA, July 10, 2014, http://www.justice.gov/dea/divisions/sd/2014/sd071014.shtml.

[37] The Sinaloa Cartel also must counter the emerging threat posed by the Cártel de Jalisco Nueva Generación (Jalisco New Generation Cartel), which is currently challenging Los Zetas in Guadalajara. *See Jalisco Cartel – New Generation (CJNG)*, INSIGHT CRIME, May 6, 2015, http://www.insightcrime.org/ mexico-organized-crime-news/jalisco-cartel-new-generation; Alasdair Baverstock, *Inside Mexico's Deadliest Cartel: How the Twisted 'New Generation' Gang – Which Took Down Army Helicopter with an RPG – is Trying to Win the Public's Heart with Ultra-Violent 'Robin Hood' Image*, DAILYMAIL.COM, May 12, 2015, http://www.dailymail.co.uk/ news/article-3077149/Inside-Mexico-s-deadliest-cartel-twisted-New-Generation-gang-took-army-helicopter-RPG-bids-win-hearts-civilians-ultra-violent-Robin-Hood-image. html.

[38] The Sinaloa Cartel's tactic of bribery first, then bullets is known as "plata o plomo" ("silver or lead"). *See* Durbin, *supra* note 18, at 32.

[39] The Sinaloa Cartel has engaged in some indiscriminate killing, however, and must not be ruled out for future consideration. *See, e.g.*, *News Report: 2008, Justice in Mexico Project*, JUSTICE IN MEXICO 1 (Trans-Border Inst. ed., Apr. 2008).

[40] *See* Peter Chalk, *Profiles of Mexico's Seven Major Drug Trafficking Organizations*, 5 CTC SENTINEL 5, 6 (2012), https://www.ctc.usma.edu/posts/profiles-of-mexicos-seven-major-drug-trafficking-organizations.

targeting Mexican civilians. Its members have engaged in beheadings, mass murders, and dismemberment, which are acts similar to those conducted by the Islamic State of Iraq and the Levant ("ISIL").[41] In regions where Los Zetas exerts its influence—in the state of Tamaulipas, for instance—the cartel continues to indiscriminately kill on a large scale,[42] decapitate victims, participate in public gunfights, and disrupting civilian life.[43] Los Zetas is currently fighting a turf war with the Sinaloa Cartel and its allies over Mexican border states, which hold key trafficking routes into the United States.[44] Because Los Zetas' actions parallel those of groups like the FARC and ISIL, this DTO qualifies for the terrorist organization designation.

3. The Gulf Cartel

The Gulf Cartel, one of the oldest DTOs in Mexico with historical ties to the Colombian Cali Cartel, is primarily located in the state of Tamaulipas.[45] This cartel previously employed Los Zetas as its military wing, but is now battling its former employee for dominance

[41] *Compare ISIS Threatens to Behead Iraq Journalist, Is Holding Others Captive*, NBC NEWS, Sept. 16, 2014, http://www.nbcnews.com/storyline/isis-terror/isis-threatens-behead-iraqi-journalist-holding-others-captive-n204226 (quoting Ziad Al-Ajily: "we are dealing with human beings who turned into monsters") *and* Alice Fordham, *Prominent Syrian Archaeologist Killed By ISIS In Palmyra*, NPR, Aug. 19, 2015, http://www.npr.org/2015/08/19/432910251/prominent-syrian-archaeologist-killed-by-isis-in-palmyra (ISIL beheading an 81-year-old archaeologist) *with* Jerry Seper, *Mexican Drug Cartel Recruiting in U.S.: Los Zetas Looks to Prisons, Street Gangs*, THE WASH. TIMES (July 7, 2013), http://www.washingtontimes.com/ news/2013/jul/7/ ruthless-mexican-drug-cartel-recruiting-in-the-us/?page=all.

[42] *See Aumenta a 193 los Muertos por Matanza en San Fernando, Tamaulipas: PGR*, ZÓCALO SALTILLO, July 6, 2011, http://www.zocalo.com.mx/seccion/articulo/ aumenta-a-193-los-muertos-por-matanza-en-san-fernando-tamaulipas-pgr (describing a mass killing of 193 migrants in the state as well as the discovery of six other mass graves).

[43] *See* Tracy Wilkinson, *In Mexico, Tamaulipas State Residents Rise up Against Cartel Violence*, L.A. TIMES (June 19, 2014), http://www.latimes.com/world/mexico-americas/la-fg-mexico-tampico-20140619-story .html#page=1.

[44] After Los Zetas became independent in 2009, the Gulf Cartel diverted its attention from combating the Sinaloa Cartel to battling Los Zetas. *See* BEITTEL, *supra* note 25, at 18.

[45] *See id.*

in northern Mexico.[46] The cartel controls substantial territory along the Texas border and it maintains its power through bribing Mexican law enforcement officials.[47] In one instance, Gulf Cartel boss Juan García Ábrego paid the Mexican Deputy Director for the Attorney General $1.5 million per month to ensure the safety of trafficking operations.[48] While the Gulf Cartel does engage in violence to control key areas of the Texas-Mexico border and has been waging war against Los Zetas since 2008, this DTO still tends to function more akin to a traditional organized criminal syndicate. It engages in bribery with state officials and only utilizes violence against opposing cartel factions, though sometimes at the expense of bystanders.[49] Because of the manner in which the Gulf Cartel currently functions, it does not merit consideration for FTO designation.

4. Vicente Carrillo Fuentes Organization

One of the deadliest cities along the U.S.-Mexico border,[50] Ciudad Juárez is home to the notorious Vicente Carrillo Fuentes Organization ("Juárez Cartel"). Based in the border state of Chihuahua, the cartel formed after the Matamoros Cartel split into smaller factions.[51] The Juárez Cartel gained its reputation for implementing extreme terror tactics through dismembering victims'

[46] The Gulf Cartel previously formed an alliance with the Sinaloa Cartel to combat Los Zetas. *See* O'Donnell & Gray, *supra* note 18, at 33.
[47] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-1018, DRUG CONTROL: U.S. ASSISTANCE HAS HELPED MEXICAN COUNTERNARCOTICS EFFORTS, BUT TONS OF ILLICIT DRUGS CONTINUE TO FLOW INTO THE UNITED STATES 15, 17 (2007).
[48] United States v. Garcia Abrego, 141 F.3d 142, 149 (5th Cir. 1998).
[49] *Gulf Cartel*, INSIGHT CRIME, http://www.insightcrime.org/mexico-organized-crime-news/gulf-cartel-profile#modus_operandi (last visited Oct. 8, 2014).
[50] *See* THE OVERSEAS SEC. ADVISORY COUNCIL, MEXICO 2014 CRIME AND SAFETY REPORT: CIUDAD JUAREZ (2014), https://www.osac.gov/ pages/ContentReport Details.aspx?cid=15634 (explaining that there were 530 murders in Ciudad Juárez in 2013); U.S. HOUSE COMM. ON HOMELAND SEC. SUBCOMM. ON OVERSIGHT, INVESTIGATIONS, AND MGMT., 112TH CONG., A LINE IN THE SAND: COUNTERING CRIME, VIOLENCE AND TERROR AT THE SOUTHWEST BORDER 36 (Comm. Print 2012) [hereinafter A LINE IN THE SAND] ("[s]ince 2008, more than 5,300 people have been killed in [the Ciudad Juárez] conflict earning Juárez the dubious title of the most dangerous city in the world.").
[51] Bloom, *supra* note 21, at 357.

corpses,[52] car bombing Mexican and American officials,[53] and assassinating police officers.[54] The organization utilizes several smaller gangs, namely La Línea and Barrio Azteca, to carry out executions.[55] These ruthless extensions of the Juárez Cartel have helped stave off the Sinaloa Cartel from controlled regions and ensured that police and civilians did not pose a threat to their operations. Though the cartel recently lost much of its dominance in Chihuahua after the city of Ciudad Juárez hired retired lieutenant colonel Julian Leyzaola as its police chief in 2011, the organization remains a threat to the stability of northern Mexico.[56] In assessing the devastation and terror created by the Juárez Cartel in the state of

[52] The Juárez Cartel is known to dismember multiple corpses and display the severed body parts in front of elementary schools and day care centers. *See* Alejandro Martínez-Cabrera & Daniel Borunda, *Dismembered Bodies Found all over Juárez*, EL PASO TIMES (Oct. 26, 2011), http://www.elpasotimes.com/ ci_19190390.

[53] *See* Press Release, Dep't of Justice, Barrio Azteca Lieutenant Who Ordered the Consulate Murders in Ciudad Juarez Found Guilty on All Counts (Feb. 19, 2014), http://www.justice.gov/opa/pr/barrio-azteca-lieutenant-who-ordered-consulate-murders-ciudad-juarez-found-guilty-all-counts; *Police: Car Bomb in Mexican Border Town Kills 4*, CNN, July 17, 2010, http://edition.cnn.com/2010/WORLD/america/07/16/mexico.juarez.explosion/?hpt=Sbin#fbid=KxD1dx2nuoa&wom=false (quoting municipal police spokesman Jacinto Seguro) ("[t]hey put him in a civilian car but dressed him up in a municipal police uniform. That's when the bomb went off. It's like an act of terrorism.").

[54] *See* Jason McGahan, *The Juarez Cartel Goes on Trial in El Paso*, TEX. OBSERVER (Feb. 21, 2014), http://www.texasobserver.org/juarez-cartel-goes-trial-el-paso/.

[55] *See* Affidavit in Support of Criminal Complaint at 4, United States v. Castrellon, No. 3:10-cr-02213 (W.D. Tex. Aug. 18, 2010); RICARDO C. AINSLIE, THE FIGHT TO SAVE JUÁREZ: LIFE IN THE HEART OF MEXICO'S DRUG WAR 82-87 (2013).

[56] *See* Stastna, *supra* note 31. After Leyzaola assumed his new position, the Juárez Cartel stated that "si [él] no se iba, mataban a un policía al día" ("if he does not leave, a police officer would be killed a day"). *See Cártel Ordena la Ejecución de un Policía al Día en Juárez*, TERRA, Jan. 27, 2012, noticias.terra.com.mx/mexico/seguridad/cartel-ordena-la-ejecucion-de-un-policia-al-dia-en-juarez,312c076313125310VgnVCM10000098f154d0RCRD.html?icid=Publicadores_Links_Relacionados; *see also* Randal C. Archibold, *Ex-Police Chief in Mexico Known for Crackdowns Is Shot*, N.Y. TIMES (May 8, 2015), http:// www.nytimes.com/2015/05/09/world/americas/ex-police-chief-in-mexico-known-for-crackdowns-is-shot.html?_r=0 (explaining that Leyzaola, known for controversial crackdowns in Ciudad Juárez, was shot by hitmen on May 8, 2015).

Chihuahua, this DTO must be considered for the State Department's terrorist organization designation.[57]

Between these four DTOs, only Los Zetas and the Juárez Cartel display characteristics of organizations already listed as FTOs. Their brutal tactics, indiscriminate killings, and political targets reveal that these cartels pose a threat to established political institutions. Both the Sinaloa and Gulf Cartels choose to use only strategies representative of organized crime, which disqualifies them from FTO designation. Their propensity toward bribery and violence limited to enemy DTOs does not reflect the tactics and motivations made illegal by Congress under section 219. As shown in Part II, Los Zetas and the Juárez Cartel fulfill the criteria required for FTO designation.

II. DEFINING TERRORISM

In order to understand the necessity of designating Los Zetas and the Juárez Cartel as terrorist organizations, it is important to analyze the definitions of "terrorism" and "terrorist activity," as defined by section 960a of the Controlled Substances Act, and section 219 of the Immigration and Nationality Act. Part II examines section 960a and section 219 independently to assess the qualifications necessary for a cartel's designation as an FTO.

A. Qualifications Under Section 960a

The Controlled Substances Act contains a small but powerful section appropriately referred to as the "Narcoterrorism Statute."[58] The actual title of section 960a is "Foreign terrorist organizations, terrorist persons and groups." It details both the acts prohibited, and the jurisdictional elements an individual must meet in order to be

[57] For the remainder of this Comment, references to the Juárez Cartel include the La Línea and Barrio Azteca gangs. These gangs function as military arms for the Juárez Cartel and conduct indiscriminate killings, extortion, and other terroristic activities. *See* Affidavit, *supra* note 55, at 4; Ainslie, *supra* note 55, at 82-87.

[58] *See, e.g.*, Michael Jacobson & Matthew Levitt, *Tracking Narco-Terrorist Networks: The Money Trail*, 34 THE FLETCHER F. OF WORLD AFF. 117, 121 (2010).

successfully convicted in U.S. federal court under U.S. federal law. The Act reads:

> (a) Prohibited acts
>
> Whoever engages in conduct…if committed within the jurisdiction of the United States, or attempts or conspires to do so, knowing or intending to provide, directly or indirectly, anything of pecuniary value to any person or organization that has engaged or engages in terrorist activity (as defined in section 1182(a)(3)(B)…) or terrorism (as defined in section 2656f(d)(2)…), shall be sentenced to a term of imprisonment of not less than twice the minimum punishment under section 841(b)(1), and not more than life, a fine…, or both…
>
> (c) Proof requirements
>
> To violate subsection (a), a person must have knowledge that the person or organization has engaged or engages in terrorist activity (as defined in section 1182(a)(3)(B)…) or terrorism (as defined in section 2656f(d)(2)…).[59]

These definitions are critical in understanding how a person violates section 960a because the terms "terrorism" and "terrorist activity" differ under various titles of the U.S. Code.[60] The question of whether these groups fall under these definitions begins with a textual analysis of the statute. For section 960a to apply to Los Zetas or the Juárez Cartel, these DTOs must assist an organization or individual engaging in either "terrorism" or "terrorist activity." DOJ may use either of these definitions to describe a cartel member in a section 960a criminal proceeding if both DTOs are added to the FTO list. The FTO designation allows DOJ to more easily prosecute members of Los Zetas and the Juárez Cartel as narcoterrorists because the FTO list unifies the perspectives of all federal agencies about certain organizations.[61]

---

[59] 21 U.S.C. § 960a(a) (2006).

[60] *See, e.g.*, GREGORY E. MAGGS, TERRORISM AND THE LAW: CASES AND MATERIALS 1 (2d. ed. 2010) (explaining that at least 22 different definitions exist for terrorism in federal law).

[61] *See infra* Part II(b)-(c).

The definition for "terrorism" is relatively short, but contains several crucial elements describing the precise nature of the crime. The definition in 22 U.S.C. § 2656f (d)(2) explains that terrorism is "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents."[62] Moreover, under Title 22 of the U.S. Code this definition of terrorism has remained the same since 1996. [63] The fact that Congress has not altered this definition in nearly two decades indicates the definition is relatively settled.

To properly apply the definition of "terrorism" to both Los Zetas and the Juárez Cartel, one must determine if these cartels fit each individual criterion in section 2656f(d)(2). An organization must meet four elements: (1) premeditation; (2) politically motivated violence; (3) perpetrated against noncombatants; and (4) performed by subnational groups or clandestine agents.

Regarding the qualification of subnational groups or clandestine agents, both Los Zetas and the Juárez Cartel easily meet this criterion because they are not branches of the Mexican government. Their violent acts are also premeditated, as they conduct planned assassinations and strategically dismember their victims to display their ruthlessness, aggression, and dominance.[64] Furthermore, both of these DTOs engage in acts against noncombatants.[65]

Thus, the sole remaining issue is whether Los Zetas and the Juárez Cartel are politically motivated when they target citizens, political officials, and police. Although these groups initially formed to enter the lucrative illegal narcotics trade, Los Zetas and the Juárez Cartel evolved into organizations whose mission is to actively disrupt

---

[62] 22 U.S.C. § 2656f(d)(2) (2004).
[63] *See* 22 U.S.C. § 2656f(d)(2) (1996).
[64] *See, e.g.*, *Mexican Drug Cartel Hitman Tells How he Committed 800 Murders Before he Stopped Keeping Track*, DAILYMAIL.COM, Feb. 11, 2014, http://www.dailymail.co.uk/news/article-2557171/ Mexican-drug-cartel-hitman-says-committed-800-murders-stopped-keeping-track.html.
[65] *See, e.g.*, Martínez-Cabrera & Borunda, *supra* note 52; Wilkinson, *supra* note 43. This factor necessarily excludes cartels like the Sinaloa Cartel and the Gulf Cartel because they tend to direct their violence toward enemy cartels and officials that pose a significant threat to their operations.

and overthrow the Mexican government by utilizing terrorist tactics. For this reason, both DTOs necessarily fulfill the politically motivated requirement.[66]

The actions conducted by Los Zetas and the Juárez Cartel fall under section 1182(a)(3)(B)'s definition of "terrorist activity." The statute lists multiple acts that constitute terrorist activity. These acts include: sabotaging vehicles; seizing or threatening to kill individuals to compel a third party (including governmental agencies) to do or abstain from an act; assassination; violently attacking an internationally protected person; using a firearm with the intent to danger one or multiple persons; or threatening to commit any of the aforementioned acts.[67] Given the previously described actions of both DTOs, it is rational to conclude that both commit "terrorist activity" for the purposes of section 1182(a)(3)(B).

Since Los Zetas has committed all of the acts listed in 22 U.S.C. § 2656f(d)(2), the DTO engages in "terrorist activity" as defined in section 1182(a)(3)(B). First, Los Zetas has engaged in kidnapping for both monetary and intimidation purposes.[68] For example, in June 2013, Mexican soldiers located and rescued 165 migrant workers abducted by Los Zetas.[69] These kidnappings also occur on American soil, with border states experiencing abductions more frequently than non-border states.[70] This DTO also engages in firefights on the streets of Tamaulipas[71] and assassinates police and government officials.[72] Furthermore, the cartel has utilized fragmentation grenades against

[66] Part IV deals exclusively with the issue of political motivation exemplified by Los Zetas and the Juárez Cartel.
[67] *See* Inadmissible Aliens, 8 U.S.C. § 1182(a)(3)(B)(iii) (2013).
[68] *See, e.g.*, Deborah Hastings, *Soldiers Rescue 165 People Brutally Kidnapped in Mexico—Adults and Children Held Terrified for Weeks at Gunpoint*, NY DAILY NEWS (June 6, 2013, 4:21 PM), http://www. nydailynews.com/news/world/soldiers-tamaulipas-mexico-rescue-165-migrants-central-america-kidnapped-organized-crime-article-1.1365304 (explaining that Los Zetas kidnaps migrants for ransom and prostitution).
[69] A LINE IN THE SAND, *supra* note 50, at 26-27.
[70] *See id.*
[71] *See* Wilkinson, *supra* note 43.
[72] For example, Los Zetas tortured and killed Cancún's tactical police operations commander Martínez Góngora in 2008. *News Report: 2008, Justice in Mexico Project*, *supra* note 39, at 4.

large groups of Mexicans celebrating national holidays.[73] Second, Los Zetas members often threaten to kill any person perceived to be in the way of their operations, mutilate bodies, and leave messages by the remains of their victims, warning Mexican civilians and other DTOs to "[s]ee. Hear. Shut up, if you want to stay alive."[74] In addition, since the escalation of cartel violence began during the Calderón presidency, the use of car bombs in Mexico has increased exponentially.[75] Los Zetas, a major contributor to this phenomenon, is responsible for detonating at least one car bomb on January 22, 2011, and is linked to two others.[76]

Members of Los Zetas have also murdered U.S. agents and personnel. On February 15, 2011, Los Zetas members ambushed and gunned down U.S. Immigration and Customs Enforcement Agent Jaime Zapata and injured his partner Victor Avila, Jr., despite Zapata and Avila identifying themselves as U.S. agents while driving a vehicle with diplomatic plates.[77] This is but one example of where Los Zetas murdered internationally protected persons in cold blood.[78] These actions are illustrative of Los Zetas' ability to successfully conduct "terrorist activity" as defined in section 1182(a)(3)(B).

The Juárez Cartel also engages in "terrorist activity" because its members currently commit or previously engaged in all of the acts outlined in the statute. In addition to routine assassinations, kidnappings, and death threats,[79] this DTO is responsible for the triple homicide in 2010, of U.S. Consulate employee Leslie Enriquez, her

---

[73] *See* ROBERT J. BUNKER & JOHN P. SULLIVAN, CARTEL CAR BOMBINGS IN MEXICO 14 (Strategic Studies Inst. ed., 2013) (referring to the attack in September 2008 on Mexicans celebrating Mexican Independence Day in the city of Morelia, which resulted in 8 deaths and 101 injuries).

[74] Los Zetas wrote this quote in the Mexican town of Reynosa next to the butchered torsos and severed heads of its victims. *See* Jerry Seper, *supra* note 41.

[75] *See* BUNKER & SULLIVAN, *supra* note 73, at 13-14.

[76] *See id.* at 18.

[77] *Id.*

[78] *See* Murder or Manslaughter of Foreign Officials, Official Guests, or Internationally Protected Persons, 18 U.S.C. § 1116(b)(4)(B) (1996) (defining "internationally protected person" as "any other…officer…or agent of the United States Government…who at the time and place concerned is entitled pursuant to international law to special protection against attack…").

[79] *See e.g.*, Press Release, Dep't of Justice, *supra* note 53; Wilkinson, *supra* note 43.

husband Arthur Redelfs, and Jorge Salcido, the husband of another Consulate employee.[80] Several months after these murders, La Línea, acting on behalf of the Juárez Cartel, constructed a car bomb to use against federal police in Ciudad Juárez.[81] The gang premeditated this attack by "dressing a bound, wounded man in a police uniform and call[ed] in a false report of an officer shot…" and then detonated the car bomb, killing the decoy and several others.[82]

Torture and murder are not new practices for the Juárez Cartel. The cartel's use of "terrorist activity" was prevalent in the infamous 2004, "House of Death" murders, where cartel members abducted, tortured, and killed nearly 20 individuals and buried their remains in Ciudad Juárez.[83] One of the victims of this atrocity, Luis Padilla, was abducted after leaving his home in El Paso, bound with duct tape, and tortured to death.[84] These targeted killings of internationally protected personnel, citizens, and political figures reveals that the definition of "terrorist activity" defined in section 1182(a)(3)(B) applies to the Juárez Cartel.

In reexamining the text of section 960a, a person engaging or attempting to aid a person or organization engaging in either "terrorism" *or* "terrorist activity" by manufacturing, distributing, or dispensing controlled substances violates the Narcoterrorism Statute.[85] This clearly indicates that the individual or group participating in the trafficking of illegal substances must assist *either* an individual or organization engaging in "terrorism" *or* an individual or organization engaging in "terrorist activity." This standard is easier to meet than a standard requiring a trafficker to engage or assist in the execution of both terrorism and terrorist activity. Since Los Zetas and the Juárez Cartel sell and manufacture illegal narcotics while simultaneously engaging in violence against political figures and

[80] *See* Press Release, Dep't of Justice, *supra* note 53. These U.S. citizens are also "internationally protected person[s]" under Title 18 of the U.S. Code. *See* 18 U.S.C. § 1116(b)(4).
[81] *See* BUNKER & SULLIVAN, *supra* note 73 at 15-16.
[82] *Id.* at 16.
[83] *See* Complaint at 16, Padilla v. United States, No. 3:05-cv-00478 (2005).
[84] *See* Affidavit of Janet Padilla at 143, Padilla v. United States, No. 3:05-cv-00478 (2006).
[85] 21 U.S.C. § 960a(a) (2006).

citizens, these cartels participate in *both* "terrorism" and "terrorist activity," and thus qualify for section 960a jurisdiction.

B. Qualifications Under Section 219 of the Immigration and Nationality Act

The plain language of section 960a supports the conclusion that Los Zetas and the Juárez Cartel assist organizations, i.e. themselves, in facilitating both "terrorism" and "terrorist activity" through the trafficking of narcotics. Yet, these DTOs are not members of the State Department's FTOs List.[86] As long as Los Zetas and the Juárez Cartel remain off of this list, any criminal actions brought under section 960a against extradited cartel members may fail. In choosing to not recognize these DTOs as terrorist groups, the executive branch implicitly undermines any claims brought against extradited cartel members for section 960a offenses. To ensure courts do not dismiss narcoterrorism suits against members of Los Zetas and the Juárez Cartel for jurisdictional reasons, the Secretary of State must place these DTOs on the FTO list. This requires the Secretary to find:

> (A) the organization is a foreign organization;
>
> (B) the organization engages in terrorist activity (as defined in section 1182(a)(3)(B)…or terrorism (as defined in section 2656f(d)(2)…) or retains the capability and intent to engage in terrorist activity or terrorism); and
>
> (C) the terrorist activity or terrorism of the organization threatens the security of United States nationals or the national security of the United States.[87]

The language of section 219 of the Immigration and Nationality Act suggests Congress contemplated that the Secretary might determine DTOs like Los Zetas and the Juárez Cartel to be terrorist organizations.[88] The criteria in section 219 are almost

[86] *See Foreign Terrorist Organizations*, *supra* note 15.
[87] 8 U.S.C. § 1189(a)(1)(A)-(C) (2004).
[88] "[T]his bill says that whether you are a member of or assisting a drug cartel along the border that employs terrorist tactics to protect its drug trade…this bill targets

identical to those used in section 960a for deciding what conduct establishes terrorism.[89] As in the section 960a analysis, Los Zetas and the Juárez Cartel fulfill the foreign organization requirement and the requirement of engaging in "terrorist activity," defined in 8 U.S.C. § 1182(a)(3)(B), or "terrorism," defined in 22 U.S.C. § 2656f(d)(2).

Having established that Los Zetas and the Juárez Cartel satisfy factors (A) and (B) of section 219, the Secretary need only determine whether the conduct of Los Zetas and the Juárez Cartel threatens U.S. national security or the security of U.S. nationals. Given both cartels' actions—supplying the United States with illegal narcotics (interfering with interstate commerce), abducting Mexicans and Americans in the United States, killing personnel working for U.S. agencies, and generally disrupting the U.S.-Mexico border—this should not be a difficult determination to make.[90] These cartels have even recruited American gang members and U.S. military personnel to serve as "hitmen" and drug runners in the United States and Mexico.[91] Also, Los Zetas and the Juárez Cartel operate in at least 3,000 American cities.[92] Furthermore, the operations and tactics of Los Zetas and the

you." 151 CONG. REC. S9835, S9846 (daily ed. Sept. 8, 2005) (statement of Sen. Cornyn).

[89] *See* 21 U.S.C. § 960a(a) (2006).

[90] *See, e.g.*, Affidavit, *supra* note 55, at 4; A LINE IN THE SAND, *supra* note 50, at 26-27; Hastings, *supra* note 68; McGahan, *supra* note 54.

[91] The FBI has reported that Los Zetas contracted with the Texas Mexican Mafia as early as 2010. *See* Memorandum for the FBI: Los Zetas' Reliance on Non-Traditional Associates May Pose Threat to the United States, (Feb. 4, 2011) (on file with FBI San Antonio Office). Former Army First Lieutenant Kevin Corley, Army Sergeant Samuel Walker, and five other Americans received jail sentences for conspiracy to function as "hitmen" for Los Zetas. *See* United States v. Corley, No. 5:12 cr 185 (S.D. Tex. Feb. 28, 2012). Army Private First-Class Michael Apodaca received a life sentence for killing Jose Daniel Gonzalez-Galeana for the Juárez Cartel after the cartel paid him $5,000. *See* Michael B. Kelley, *Mexican Cartels Are Recruiting US Soldiers as Hitmen, and the Pay Is Good*, BUS. INSIDER, Aug. 5, 2013, http://www. businessinsider.com/cartels-are-recruiting-us-soldiers-as-hitmen-2013-8.

[92] Other cartels currently not under consideration for the terrorist organization assignment by this Comment also operate in the U.S. *Mexican Drug Cartels Outgunning Law Enforcement Across the U.S. – Not just near the Border – and have Infiltrated 3,000 Cities, Sheriffs Warn*, DAILYMAIL.COM, Apr. 13, 2014, http:// www. dailymail.co.uk/news/article-2603819/Mexican-drug-cartels-outgunning-law-enforcement-U-S-not-just-near-border-infiltrated-3-000-cities-sheriffs-warn.html.

Juárez Cartel threaten American security along the U.S.-Mexico border and within U.S. non-border states. The Secretary need only consider these facts to determine that the last criterion of section 219 is fulfilled.

C. The Benefits of Section 960a and Section 219 Designation

Applying section 219 FTO designation to Los Zetas and the Juárez Cartel to help prosecute cartel members for violating section 960a would be significant in combating cartel violence. For example, once a DTO becomes a designated FTO under section 219, the Department of the Treasury may force U.S. financial institutions to block the financial assets of the DTO.[93] This is important for combating Mexican cartels because of their previous utilization of major banking firms like HSBC and Bank of America in financing their activities.[94] With the section 219 designation, Los Zetas and the Juárez Cartel will face added obstacles to laundering money through legitimate sources to fund their operations.

While section 219 would grant the U.S. federal government the authority to freeze Los Zetas and the Juárez Cartel's assets, the government already holds the ability to do so under the Foreign Narcotics Kingpin Designation Act ("Kingpin Act"). Under the Kingpin Act, the U.S. government shall "apply economic and other financial sanctions to significant narcotics traffickers and their organizations worldwide…."[95] The federal government has used the Kingpin Act to place sanctions on Los Zetas as recently as February 2014.[96]

---

[93] 8 U.S.C. § 1189(a)(2)(C) (2004).

[94] In 2012, HSBC paid $1.9 billion in fines to the U.S. Treasury for laundering money for the Sinaloa and the Colombian Norte del Valle cartels. *See* Carrick Mollenkamp, *HSBC Became Bank to Drug Cartels, Pays Big for Lapses*, REUTERS, Dec. 12, 2012, http://uk.reuters.com/article/2012/12/12/us-hsbc-probe-idUSBRE8BA05M20121212; Miguel Angel Trevino Morales, a major leader of Los Zetas, was indicted for laundering over $1 million through Bank of America. *See* Indictment at 15, United States v. Trevino, No. 1:12-cr-00210-SS (W.D. Tex. May 30, 2012).

[95] Findings and Policy, 21 U.S.C. § 1901(b) (1999).

[96] *See* Press Release, Dep't of the Treasury, Treasury Expands Sanctions Against the Los Zetas Drug Cartel (Feb. 14, 2014), http://www.treasury.gov/press-center/press-

One might question the purpose of section 219 designation given the U.S. government's use of the Kingpin Act to undermine the financial stability of Los Zetas. However, section 219 designation is significant for purposes other than applying sanctions. It is an essential tool for extraditing members of Los Zetas and the Juárez Cartel for section 960a violations. When an organization becomes an FTO under section 219, all relevant executive agencies recognize the organization as such, which clarifies any issues regarding the organization's legal status.[97] Agencies like the Departments of State, Treasury, Justice, and Homeland Security all recognize the FTO list and act in unison against those groups on the FTO list.[98] The executive branch's unified recognition of Los Zetas and the Juárez Cartel as terrorist organizations alleviates obstacles for prosecutors pursuing terrorist charges against cartel members.

Furthermore, section 219 designation eases the government's ability to extradite members of Los Zetas and the Juárez Cartel to the United States for prosecuting section 960a violations. As explained, these cartels pose a major threat to U.S. national security.[99] Through the use of section 960a, those cartel members convicted face mandatory increased prison sentences and may be deterred from participating in cartel activities in the future.[100]

releases/Pages/jl2254.aspx. Los Zetas was added to the list of drug kingpins under the Drug Kingpin Act on April 15, 2009. *See* Fact Sheet, The White House, Overview of the Foreign Narcotics Kingpin Designation Act (Apr. 15, 2009), https://www. whitehouse.gov/the-press-office/fact-sheet-overview-foreign-narcotics-kingpin-designation-act.

[97] AUDREY KRUTH CRONIN, CONG. RESEARCH SERV., RL32120, THE "FTO LIST" AND CONGRESS: SANCTIONING DESIGNATED FOREIGN TERRORIST ORGANIZATIONS 7 (2003).

[98] *Id.*

[99] *See, e.g.*, BEITTEL, *supra* note 25, at 22; Press Release, Dep't of Justice, *supra* note 53; Anthony Kimery, *Shots That Forced Down CBP Helicopter Not The First Time A CBP Chopper Brought Down*, HOMELAND SECURITY TODAY, June 8, 2015, http://www.hstoday.us/single-article/shots-that-forced-down-cbp-helicopter-not-the-first-time-a-cbp-chopper-brought-down/00dcaab8ebb0a196d9f847c1f3d1e28c.html (reporting on an emergency landing by a Customs and Border Protection helicopter in Laredo, Texas after taking fire from drug traffickers located in the Los Zetas stronghold of Nuevo Laredo, Mexico).

[100] Section 960a automatically doubles the minimum punishment under 21 U.S.C. § 841(b)(1), with a maximum sentence of life. 21 U.S.C. § 960a(a) (2006). Under

The Narcoterrorism Statute automatically increases the mandatory minimum sentences for selling or manufacturing narcotics to support a terrorist organization.[101] This automatic provision does not limit a court from implementing a harsher jail sentence if it determines that the offender's actions warrant a longer incarceration. Violators of section 960a face the possibility of a court increasing their base offense level by 12 through the terrorism enhancement provision located in the U.S. Sentencing Commission Guidelines Manual.[102] For the terrorism enhancement provision to apply, an organization must engage in the "[f]ederal crime of terrorism," which is defined as any offense "calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct."[103] In at least one section 960a case, the U.S. Court of Appeals for the District of Columbia upheld the use of the terrorism enhancement provision in sentencing a person engaging in narcoterrorism.[104]

Most importantly, when an organization receives, section 219 FTO designation, a defendant facing criminal action cannot challenge the organization's FTO designation either before or after trial.[105] Without the ability to challenge Los Zetas or the Juárez Cartel's FTO designation, cartel members or cartel affiliates cannot escape prosecution by disputing whether these cartels commit acts of terrorism. Without having to prepare for long arguments over

§ 841(b)(1), any person dealing vast quantities of illegal substances like heroin or cocaine automatically receive a minimum of ten years in prison, and automatically receives twenty years if death or serious bodily injury resulted from using the substance. Prohibited Acts A, 21 U.S.C. § 841(b)(1)(A) (2010).

[101] 21 U.S.C. § 960a(a) (2006).

[102] U.S. SENTENCING COMMISSION GUIDELINES MANUAL § 3A1.4 (U.S. SENTENCING COMM'N 2014). The Sentencing Table in the Manual explains the system of incarceration levels for various criminal activities. The terrorism enhancement section of the Manual allows a court to increase the base offense level by 12 if it deems this to be appropriate. *See* U.S. SENTENCING COMMISSION GUIDELINES MANUAL § 5, pt. A, sentencing table (U.S. SENTENCING COMM'N 2014).

[103] Acts of Terrorism Transcending National Boundaries, 18 U.S.C. § 2332b(g)(5)(A) (2008). *See infra* Part IV for in-depth analysis on the matter of government coercion, intimidation, and retaliation against both the Mexican and American governments.

[104] *See* United States v. Mohammed, 693 F.3d 192, 201 (D.C. Cir. 2012).

[105] 8 U.S.C. § 1189(a)(8) (2004).

whether Los Zetas or the Juárez Cartel commit terrorism, prosecutors can focus their efforts on finding evidence in support of section 960a charges.

The D.C. Court of Appeals already recognizes the legitimacy and value of using section 960a by law enforcement personnel. In *United States v. Mohammed*, the court recognized the fact that penalties under section 960a surpass those for drug trafficking and material support combined.[106] This did not deter the court from upholding the lower court in finding that Khan Mohammed, a Taliban affiliate, violated section 960a when he sought to fund the construction of a car bomb to be used at a NATO airbase with drug profits.[107] The court explained that Mohammed could not argue section 960a failed to apply in his case because he lacked the intent to finance terrorism with drug sales.[108] The language of the statute fails to include a *mens rea* requirement and is unambiguous as to when it applies. A person violates section 960a when he directly or indirectly supports terrorism through selling, manufacturing, distributing, or dispensing illegal narcotics.[109] The court explicitly stated that Congress intended to ensure the Narcoterrorism Statute extended to those using narcotics to further terrorism violate section 960a, regardless of whether they knew the profits would directly fund terrorist attacks.[110] The person need only assist the terrorist organization with the sale or supply of narcotics.[111]

Using a criminal scheme of higher mandatory minimum sentences and increased apprehensions for narcoterrorism could deter cartel members on the margin from further engaging in cartel violence. The theory of general deterrence explains that the criminal law can make citizens law abiding with the right incentive structure.[112] Though most Los Zetas and Juárez Cartel members are not U.S.

---

[106] *Mohammed*, 693 F.3d at 199-200.
[107] *Id.* at 195.
[108] *Id.* at 199.
[109] 21 U.S.C. § 960a(a) (2006). *See also* 21 U.S.C. § 841(a) (2010).
[110] *Mohammed*, 693 F.3d at 199-01.
[111] *Id.* at 201.
[112] J. ANDENAES, PUNISHMENT AND DETERRENCE 7 (Ann Arbor: Univ. of Mich. ed., 1974).

citizens, the general deterrence theory does apply to those who are subject to the punishments of the law. Merely increasing mandatory minimum sentences will not likely deter cartel members if there is no added risk of apprehension. Criminals who perceive an increased certainty of punishment associated with their illicit conduct tend to avoid these activities more often than if there is an increase in severity of the punishment.[113] By designating these cartels as terrorist organizations while also implementing a policy of rigorous extradition with heightened prison sentences, cartel members on the margin could be deterred from engaging in illegal and violent activities.

This is not to say that the law will deter most members of Los Zetas and the Juárez Cartel. The culture and nature of cartel life is reminiscent of an intimate family, where pride and unity are valued over legal repercussions.[114] Both Los Zetas and the Juárez Cartel embrace the idea of narcoculture and base their entire personal and social identification framework on this concept.[115] Both DTOs incorporate spiritual symbols like Santa Muerte, or Saint Death, into cartel folklore, which may explain why members engage in heinous acts of violence.[116] Santa Muerte serves as a source of spiritual motivation and courage, thus supplementing the narcoculture of violence and death.[117] For these cartel members, the cult-like atmosphere of Los Zetas and the Juárez Cartel outweighs a heightened probability of capture and severe incarceration sentence. However, deterrence may be possible for those individuals considering whether to join one of these organizations. Deterrence may also be possible for those current cartel members who are not yet completely engulfed in narcoculture.

---

[113] VALERIE WRIGHT, DETERRENCE IN CRIMINAL JUSTICE: EVALUATING CERTAINTY VS. SEVERITY OF PUNISHMENT 4 (The Sentencing Project ed., 2010).

[114] *See generally* Paul Wood, *Inside Mexico's Feared Sinaloa Drugs Cartel*, BBC NEWS, May 16, 2014, http://www.bbc.com/news/magazine-27427123; Tony M. Kail, *The Narco Cult of Santa Muerte*, 16 J. OF COUNTERTERRORISM & HOMELAND SECURITY INT'L 40, 40-42 (2005).

[115] *See* Kail, *supra* note 114, at 41.

[116] *Id.* Santa Muerte is seen as a spiritual guide and a symbol of courage. *Id.* For cartels, Santa Muerte serves as a guide for spiritual courage in committing severe acts of violence. *See id.* at 45.

[117] *See id.*

III. APPLICATION - THE FUERZAS ARMADAS REVOLUCIONARIAS DE COLOMBIA

To better understand the benefits of prosecuting members or affiliates of terrorist organizations under section 960a, it is useful to examine how U.S. prosecutors have already specifically referenced section 219 FTO designation in support of section 960a prosecutions. The FARC serves as a proper case study, as the FTO is located in Latin America and has traditionally participated in the illegal drug trade. The FARC serves as a better example for comparison with Mexican DTOs than Islamic terror groups like al-Qaeda because the FARC is not motivated by religion in waging war against Colombia, killing civilians, or maiming political figures.

Established in 1964, the FARC is a Marxist-Leninist guerrilla group based in Colombia.[118] Secretary of State Madeline Albright designated the FARC as a terrorist organization in 1997,[119] pursuant to section 219 of the Immigration and Nationality Act because of its repeated efforts to overthrow the Colombian government, and for killing Americans and destroying American property abroad.[120] The FARC carried out these attacks against Americans in retaliation for assisting the Colombian government in combating FARC operations.[121] The FARC previously maintained ties with other terrorist organizations, including the Irish Republican Army, who shared knowledge on constructing explosive devices.[122] The FARC has also conducted bombing campaigns against the Colombian government, police officers, and American civilians. Moreover, the

[118] ENCYCLOPEDIA OF THE DEVELOPING WORLD 1362 (Thomas M. Leonard ed., 3d vol. 2006).
[119] Fact Sheet, Dep't of State, Secretary of State designates Foreign Terrorist Organizations (FTO's) (Oct. 1, 2001), http://20012009.state.gov/r/pa/prs/ps/2001/5265.htm.
[120] United States v. Issa, No. 1:09-cr-01244-BSJ, 2 (S.D.N.Y. Dec. 30, 2009).
[121] *Id.*
[122] *See Revolutionary Armed Forces of Colombia*, GLOBALSECURITY.ORG, http://www.globalsecurity. org/military/world/para/farc.htm (last visited Sept. 15, 2015).

group is notorious for assassination attempts on major Colombian political figures.[123]

The FARC funds its operations predominantly through cultivating coca plants to make cocaine, and generates between $200 and $400 million annually in revenue.[124] The FARC has diversified its sources of revenue by expanding into the illegal markets of prostitution, kidnapping, extortion, and rural farming taxation schemes.[125] Though it began predominantly as an ideological group, the FARC evolved into a major cocaine trafficking organization, and implemented terroristic tactics in order to further its lucrative narcotics operation.[126] The FARC slowly evolved from a politically motivated organization to one focused on both narcoprofits and political intimidation.

To counter this narcoterrorism threat, the U.S. government extradited José María Corredor-Ibague to the United States for violating section 960a.[127] During a grand jury hearing, the grand jury accused Corredor-Ibague of controlling airstrips used to transport cocaine between Venezuela and Colombia in exchange for high caliber firearms.[128] In its first charge against Corredor-Ibague, the grand jury emphasized that the FARC was an FTO under section 219 of the Immigration and Nationality Act.[129] In acknowledging the FARC's location on the State Department's FTO list, the grand jury demonstrated that no question existed as to the validity of charging a person with assisting the FARC in trafficking cocaine under

---

[123] In 2002, newly elected President Álvaro Uribe Vélez survived mortar shells during his inauguration in Bogotá. *See, e.g.*, Juan Forero, *Explosions Rattle Colombian Capital During Inaugural*, N.Y. TIMES (Aug. 8, 2002), http://www.nytimes.com/ 2002/ 08/08/world/explosions-rattle-colombian-capital-during-inaugural. html.

[124] ENCYCLOPEDIA OF THE DEVELOPING WORLD, *supra* note 118, at 1362.

[125] *Id.*

[126] Donnie Marshall, *Narco-Terrorism: The New Discovery of an Old Connection*, 35 CORNELL INT'L L.J. 599, 602 (2002).

[127] Corredor-Ibague was the first person to be indicted for violating section 960a. *See* Thomas, Jr., *supra* note 16, at 1889.

[128] Indictment at 4, United States v. Corredor-Ibague, No. 1:06-cr-00344 (2006), http://counterterrorismblog.org/newslinks/upload/2008/10/us_two_colombians_ arraigned_in/Boyaco_Terror_Indictment_113006%5B1%5D.pdf (indictment issued by the grand jury).

[129] *Id.* at 2.

section 960a. The Corredor-Ibague grand jury case illustrates the necessity of section 219 designation in charging an individual under section 960a. Without the FARC's inclusion on the FTO list, the possibility existed that the grand jury would have deemed section 960a inapplicable.

In September 2013, the United States District Court for the District of Columbia found Corredor-Ibague guilty of assisting the FARC in selling cocaine to materially support the group's terrorist campaign under section 960a.[130] In approving Corredor-Ibague's 16-year jail sentence, Acting Assistant Attorney General Raman, one of the case's prosecutors, explained that this unprecedented ruling demonstrated the Justice Department's commitment to incarcerate supporters of narcoterrorism.[131] The case is indicative of how the Narcoterrorism Statute functions when applied to terrorist groups that are not Islamic fundamentalists.

The FARC has evolved into an entity focused as much on narcoprofit as on implementing its Marxist ideology. It implements campaigns of terror against the Colombian government and its citizens to further its cocaine empire and its Marxist goals.[132] In sentencing Corredor-Ibague, the D.C. District Court referred to him as an international drug lord seeking to assist the FARC through drug sales.[133]

IV. POLITICAL MOTIVATION

The recognition of the FARC's narcoterror agenda is comparable to that of Los Zetas and the Juárez Cartel, and offers support as to why these Mexican DTOs operate in accordance

[130] *High-Level Colombian Drug Trafficker Sentenced to 194 Months in Prison*, DEP'T OF JUSTICE (Sept. 16, 2013), http://www.justice.gov/opa/pr/high-level-colombian-drug-trafficker-sentenced-194-months-prison.
[131] *Id.*
[132] Although attacks conducted by FARC occur less frequently than during the 1990s and early 2000s, the organization still seeks to further their political goals through violence. *See, e.g.*, *Colombia Farc Rebel Attack Leave 500,000 Without Power*, BBC NEWS, June 12, 2015, http://www.bbc.com/news/world-latin-america-33105398.
[133] *High-level Colombian Drug Trafficker Sentenced to 194 Months in Prison*, *supra* note 130.

with section 960a's requirement of political motivation. Though the FARC began as an organization outspoken against the Colombian government, it evolved into a group that sought to gain narcoprofits while also seeking to wage war against the state.[134] In regard to Los Zetas and the Juárez Cartel, their evolutionary history is the opposite of the FARC's: they began merely as DTOs but are now pursuing the eradication of the Mexican government in several Mexican states while waging war against American police forces.[135] Though these cartels may not expressly state that their intentions are politically motivated, their actions demonstrate that they are not only motivated in violently toppling democratically elected governments, but are successful in doing so.[136] An inquiry into the definition of "terrorism" found within section 960a reveals that Congress not only aimed to include Mexican DTOs as terrorist organizations, but also that Los Zetas and the Juárez Cartel currently display the proper political motivation necessary to be deemed FTOs.

A. Cartel Actions: More than Purely Financial Gain

The definition of "terrorism" in section 960a is "premeditated, *politically motivated* violence perpetrated against noncombatant targets by subnational groups or clandestine agents" (emphasis

---

[134] *See* ENCYCLOPEDIA OF THE DEVELOPING WORLD, *supra* note 118, at 1362-63.

[135] This eradication is apparent through the DTOs' successful disruption of political processes and social structures. *See, e.g.*, *Barrio Azteca Leader Sentenced to Life in Prison and Two Barrio Azteca Soldiers Sentenced to 20 and 30 Years in Prison*, DEP'T OF JUSTICE, June 29, 2012, http://www.justice.gov/opa/ pr/barrio-azteca-leader-sentenced-life-prison-and-two-barrio-azteca-soldiers-sentenced-20-and-30 (describing cartel tax systems); Jo Tuckman, *Leading Politician Rodolfo Torre Cantú Murdered in Mexico*, THE GUARDIAN (June 28, 2010), http://www.theguardian.com/world/2010/jun/29/leading-politician-rodolfo-torre-cantu-murdered-mexico; *Clinton Says Mexico Drug Crime like an Insurgency*, BBC NEWS, Sept. 9, 2010, http://www.bbc.com/news/world-us-canada-11234058 (Secretary of State Hillary Clinton equating Mexican DTO violence to an "insurgency").

[136] *See, e.g.*, Guadalupe Correa-Cabrera, *The Spectacle of Drug Violence: American Public Discourse, Media, and Border Enforcement in the Texas-Tamaulipas Border Region During Drug-War Times*, 7 NORTEAMÉRICA 199, 208 (2012) (quoting Representative Silvestre Reyes) ("[cartel members] frequently engage in brutal acts of narco-terrorism to undermine democratic institutions and the rule of law, and to incite fear among the people and law enforcement"); Shawn T. Flanigan, *Terrorists Next Door? A Comparison of Mexican Drug Cartels and Middle Eastern Terrorist Organizations*, 24 TERRORISM AND POLITICAL VIOLENCE 279, 285-87 (2012).

added).[137] Though section 960a applies to those persons who assist a group engaging in either "terrorist activity" or "terrorism," it is necessary to determine that both Los Zetas and the Juárez Cartel engage in terrorism to ensure that these DTOs are defined cohesively for section 219 and section 960a purposes. It is not enough to cite extreme violence by these organizations because other Mexican DTOs commit similar acts without adequate political motivations. To be considered "politically motivated" for the purposes of meeting this standard, Los Zetas and the Juárez Cartel must seek to coerce the Mexican and American governments to act in a certain way through terrorist tactics and violence.

Several experts in Mexican cartel violence argue that only profits motivate Los Zetas and the Juárez Cartel.[138] Los Zetas and the Juárez Cartel are often described as not "wish[ing] to remove the Mexican Government and replace it with one of their own…[t]hey simply want to maximize their profits and keep government…out of their business."[139] The conclusion that these DTOs are motivated only by profit overlooks the intentionality of their sheer violence against civilians and public employees, strategic targeting schemes against politicians and police, and quasi-governmental structures in controlled territories. The actions of Los Zetas and the Juárez Cartel speak louder than words and are vital in recognizing their commitment to disrupt and hamper the Mexican government.

Former Secretary of Homeland Security Michael Chertoff explained that Mexican DTOs seek to "terrorize the population of Mexico so that either [the] President…will be forced to pull back, or

---

[137] 22 U.S.C. § 2656f(d)(2) (2004).

[138] *See, e.g.*, Shawn T. Flanigan, *supra* note 136, at 285-87; *see also* Ben Jakovljevic, *Terror in Trading: Should the United States Classify Mexican Drug Trafficking Organizations as Terrorist Organizations?*, 23 S. CAL. INTERDISC. L.J. 355, 383-85 (2014).

[139] Sylvia M. Longmire & Lt. John P. Longmire, *Redefining Terrorism: Why Mexican Drug Trafficking is More than Just Organized Crime*, 1 J. OF STRATEGIC STUD. 35, 47 (2008) (arguing that organizations do not need to display political motivation to constitute as terrorist organizations, offering Autodefensas Unidas de Colombia as an example of a non-politically motivated terrorist organization).

[be] willing to make peace with the cartels."[140] This became glaringly true when members of Los Zetas assassinated gubernatorial candidate Rodolfo Torre Cantú in the state of Tamaulipas in 2010.[141] Following Cantú's assassination, more political figures and law enforcement personnel were assassinated, including twelve mayors, police officers, and military personnel.[142] In targeting and assassinating political figures, Los Zetas and the Juárez Cartel have disrupted the Mexican political process, which allows these DTOs to control vast areas of the nation for their own benefit. Killing these political and law enforcement figures allows Los Zetas and the Juárez Cartel to implement taxes that lesser illicit narcotics organizations[143] and civilians living in territory controlled by the DTOs must pay.[144] Taxation is a vital part of a state's functionality in governing its citizens. Los Zetas and the Juárez Cartel understand the importance of these taxes, and use deadly force and terror tactics to implement their own taxes and eliminate government competition for tax revenue collection. These DTOs target and kill citizens, political figures, and law enforcement not only to further drug profits, but also to function as a quasi-political state and strike fear in the Mexican and American populations.

B. Los Zetas and the Juárez Cartel: A Threat to U.S. National Security

Los Zetas and the Juárez Cartel attempt to disrupt and undermine the U.S. government in several ways. In particular, Los

---

[140] Michael Chertoff, *Keynote Address: "The Nexus Between Drug Trafficking, Terrorism and Organized Crime"*, 13 CHAP. L. REV. 681, 685 (2010).
[141] *See* Tuckman, *supra* note 135.
[142] O'Donnell & Gray, *supra* note 18, at 30.
[143] *See* Samuel Logan, *A Profile of Los Zetas: Mexico's Second Most Powerful Drug Cartel*, COMBATING TERRORISM CTR. (Feb. 16, 2012), https://www.ctc.usma.edu/posts/a-profile -of-los-zetas-mexicos-second-most-powerful-drug-cartel. *See also Barrio Azteca Leader Sentenced to Life in Prison and Two Barrio Azteca Soldiers Sentenced to 20 and 30 Years in Prison*, *supra* note 135 (explaining that Barrio Azteca extorts "quota," or taxes, on non-Barrio Azteca drug dealers).
[144] *See* GEORGE W. GRAYSON, MEXICO: NARCO-VIOLENCE AND A FAILED STATE? 82 (Transaction Publishers 2010) (describing the territory tax Mexican citizens pay to drug cartels). *See also* A LINE IN THE SAND, *supra* note 50, at 39 (2012) (explaining that Los Zetas burnt down a casino because its owners refused to pay a protection tax).

Zetas allegedly maintains ties with Hezbollah, a group the United States has recognized as an FTO since 1997.[145] Also, both DTOs have targeted and killed U.S. civilians, border patrol agents, and diplomats. The concentration of violence along the U.S.-Mexico border and the terroristic activity instigated by these DTOs toward Americans support the conclusion that Los Zetas and the Juárez Cartel should receive FTO status.

With the steady influx of Lebanese nationals immigrating to Mexico, both legally and illegally for decades, members of Hezbollah, a State Department-designated FTO, have reportedly settled in the Central American nation.[146] While Hezbollah traditionally operates out of the tri-border region of Argentina, Brazil, and Paraguay,[147] the FTO also functions in Mexico.[148] Los Zetas members and affiliates have allegedly helped Hezbollah establish residencies in Mexico, engage in illegal drug trade, launder money, and possibly enter the United States illegally.[149] In return, Hezbollah has purportedly trained cartel members in bomb construction and explosives development, and provided them with weapons.[150]

---

[145] *See Foreign Terrorist Organizations*, *supra* note 15. The extent of these ties is unknown at the time of publication for this Comment.
[146] Rosenthal, *supra* note 19.
[147] LIBRARY OF CONG., TERRORIST AND ORGANIZED CRIME GROUPS IN THE TRI-BORDER AREA (TBA) OF SOUTH AMERICA 14 (ed. 2015).
[148] *See* O'Donnell & Gray, *supra* note 18, at 32. *See also See Hezbollah in Latin America – Implications for U.S. Homeland Security: Hearing Before the Subcomm. On Counterterrorism and Intelligence*, 112th Cong. 27 (2011) [hereinafter *Hezbollah in Latin America*] (explaining that Mexico serves as a "financial conduit" for Hezbollah and that Hezbollah has infiltrated the U.S. through the "porous" southern border); LIBRARY OF CONG., *supra* note 147, at 19 (describing a Hezbollah plot to assassinate President Vicente Fox and carry out a terrorist attack against the Mexican Senate in Mexico City on October 10, 2001).
[149] Rosenthal, *supra* note 19; *Terrorist group Hezbollah is Working with Mexican Cartels (U.S. Homeland Security)*, THE YUCATAN TIMES (May 30, 2015), http://www.theyucatantimes.com/2015/03/terrorist-group-hezbollah-is-working-with-mexican-cartels-u-s-homeland-security/ (explaining that Tom Diaz, former senior policy analyst at Violence Policy Center, claims that Hezbollah is involved with drug trafficking in Mexico).
[150] *Hezbollah in Latin America*, *supra* note 148, at 1 (written testimony of Ambassador Roger T. Noriega before the Subcommittee on Counterterrorism and Intelligence).

This emerging relationship poses a major national security concern for the United States, as evidenced by by the recent attempted assassination of the Saudi Arabian ambassador in Washington D.C.[151] Mannsor Arbabsiar, an affiliate of Hezbollah and Iran's al Quds Force, attempted to hire a Los Zetas hitman to bomb a restaurant while the Saudi ambassador dined there.[152] Arbabsiar understood that the purported Los Zetas hitman would bomb the restaurant, and likely kill between 100 and 150 bystanders.[153] Any attempt by Hezbollah to use the cartel as a means to try and execute extensive terrorist attacks within the United States poses a direct threat to U.S. national security. The Arbabsiar plot indicates that Los Zetas is a potential asset for Islamic terrorist organizations seeking to act within in the Americas.

The Juárez Cartel also conducts terrorist acts against the United States and Mexican governments to alter their behavior. Through its proxy Barrio Azteca, the Juárez Cartel murdered U.S. Consulate employee Leslie Enriquez, her husband Arthur Redelfs, and Jorge Salcido, the husband of another Consulate employee.[154] Also, because the Juárez Cartel controls drug trafficking corridors through Texas, the cartel's operations are subject to the actions and influence of U.S. law enforcement. Furthermore, the Juárez Cartel seeks to remove U.S. personnel from its claimed territory in order to impose its tax plans[155] and continue drug trafficking, human smuggling, and indiscriminate migrant killings. The Juárez Cartel has a strong incentive to eliminate United States and Mexican governments from

[151] Arbabsiar v. United States, No. 14 Civ. 3222, 2014 WL 6463229, at *5 (S.D.N.Y. Nov. 18, 2014); Peter Finn, *Man in Iran-Backed Plot to Kill Saudi Ambassador Gets 25 Years*, THE WASH. POST (May 30, 2013), https://www.washington post.com/world/national-security/man-in-iran-backed-plot-to-kill-saudi-ambassador-gets-25-years/2013/05/30/0435e7a2-c952-11e2-8da7-d274bc611a47_ story.html.

[152] Reply Brief for Appellant, United States v. Ali-M Aldawsari, No. 5:11-CR-15-1 (5th Cir. 2013) (No. 12-11166), 2013 WL 4050816, at *21.

[153] *Id.* The Hezbollah affiliate contacted an undercover DEA agent posing as a member of Los Zetas and explained that he would bomb the restaurant, which would likely kill many bystanders. *Id.*

[154] *See* Press Release, Dep't of Justice, *supra* note 53.

[155] *See* Tuckman *supra* note 135. *See also* O'Donnell & Gray, *supra* note 18, at 30.

its territory, which would allow the Juárez Cartel to function as the sole authority in the greater Ciudad Juárez region.

While one stated goal of Los Zetas and the Juárez Cartel is to increase profits, their actions reveal their related goals of disrupting the U.S. and Mexican governments. The cartel was previously successful in partially overthrowing the Mexican government in cartel-controlled territories and may do so again in the future. The Juárez Cartel's activities altered the political and social frameworks within the state of Chihuahua and forced the U.S. government to respond to threats along the border. These governmental responses are enough to show that the Juárez Cartel aims to disrupt political life in Mexico and the United States. Thus, the cartel displays sufficient political motivation for FTO designation.

Upon receiving FTO designation, a Los Zetas or Juárez Cartel member, affiliate, or drug supplier need only assist Los Zetas or the Juárez Cartel in selling or cultivating illicit narcotics in order to be extradited to the United States, where they may be sentenced to lengthy incarceration in the American penal system.[156] This will aid the Mexican and American governments in combating the dangers posed by DTOs and convey that the United States deals with extreme terroristic cartel violence seriously and effectively.

V. JURISDICTIONAL CONCERNS

Though Los Zetas and the Juárez Cartel fulfill the requirements of an FTO outlined in section 219 of the Immigration and Nationality Act, the United States must also be able to assert proper extraterritorial jurisdiction over individuals assisting in selling or manufacturing illegal narcotics. Traditionally, the United States holds extraterritorial jurisdiction over an individual whose overt act outside of the United States effectuates an adverse occurrence within

[156] *See* 21 U.S.C. § 960a(a) (2006); *see also* Superseding Indictment at 4, 9, United States v. Juma Khan, No. S2 08 Cr. 621 (S.D.N.Y. 2009) (explaining that Haji Juma Khan violated 21 U.S.C. § 960a by supplying morphine base to the Taliban, a group actively engaging in terrorist activity).

American territory.[157] Jurisdiction may also extend to individuals whose conspiracy occurred outside the United States, but whose final effects were intended to occur within American territory.[158] Accordingly, when individuals seek to sell or cultivate illegal narcotics on behalf of Los Zetas or the Juárez Cartel abroad with the intent to cause an effect in the United States, the U.S. government possesses extraterritorial jurisdiction to extradite them to the United States for trial.

Two requirements must be met in order for section 960a to hold any weight in extraditing violators who are located outside U.S. territory: (1) the statute must clearly express Congress's intent for it to apply outside of the U.S.;[159] and (2) a treaty must exist between the United States and the nation in which the perpetrator is located.[160] The text of section 960a makes it clear that Congress intended to provide for U.S. jurisdiction over violators of the statute.

A. Jurisdiction in Section 960a

The statute includes the following section devoted solely to jurisdiction:

> (b) Jurisdiction. There is jurisdiction over an offense under this section if…

[157] *See, e.g.*, United States v. Postal, 589 F.2d 862, 885 (5th Cir. 1979) (stating that proof of an overt act in the U.S. creates extraterritorial jurisdiction over subsequent attempted acts abroad).

[158] Wayne R. LaFave, et al., Federal Jurisdiction, 4 Crim. Proc. § 16.4(b) (3d ed.) (describing "objective territoriality").

[159] *See* United States v. Bowman, 260 U.S. 94, 98-99 (1922) (explaining that the nature of the offense may allow Congress's intent to be inferred without a specific provision); *see also*, United States v. Martinelli, 62 M.J. 52, 61 (C.A.A.F. 2005) (explaining that a statute's language "must be clear enough to overcome a presumption that it was intended to apply domestically, not simply lend itself to a plausible argument that it applies overseas.").

[160] DEP'T OF JUSTICE, U.S. ATTORNEY'S MANUAL tit. 9 § 15.210 (2015), http://www.justice.gov/usam/usam-9-15000-international-extradition-and-related-matters#9-15.210.

> (2) the offense, the prohibited drug activity, or the terrorist offense occurs in or affects interstate or foreign commerce;
>
> (3) an offender provides anything of pecuniary value for a terrorist offense that causes or is designed to cause death or serious bodily injury to a national of the United States while that national is outside the United States, or substantial damage to the property of a legal entity organized under the laws of the United States (including any of its States, districts, commonwealths, territories, or possessions) while that property is outside of the United States;
>
> (4) the offense or the prohibited drug activity occurs in whole or in part outside of the United States (including on the high seas), and a perpetrator of the offense or the prohibited drug activity is a national of the United States or a legal entity organized under the laws of the United States (including any of its States, districts, commonwealths, territories, or possessions); or
>
> (5) after the conduct required for the offense occurs an offender is brought into or found in the United States, even if the conduct required for the offense occurs outside the United States.[161]

The language in sections 960a(b)(2)-(5) suggests Congress intended section 960a to apply to actions conducted by both citizens and noncitizens alike. Section 960a(b)(4) grants the United States jurisdiction over section 960a violations occurring both partially, and completely, outside of the United States.[162] The explicit nature of the statute's language may only be read as granting extraterritorial jurisdiction to perpetrators acting abroad.

The legislative history of section 960a also supports the notion that Congress intended to provide for extraterritorial jurisdiction. Senator John Cornyn observed, "this bill says that whether you are a member of or assisting a drug cartel along the border that employs terrorist tactics to protect its drug trade…this bill targets you."[163]

[161] 21 U.S.C. § 960a(b)(2)-(5) (2006).
[162] *Id.*
[163] 151 CONG. REC. S9835, S9846 (daily ed. Sept. 8, 2005) (statement of Sen. Cornyn).

Congressman Henry Hyde added that the statute would create "a new crime that...address[es] and punish[es] those who would use…illicit narcotics to promote and support terrorism."[164] Statements by Representatives and Senators demonstrate that Congress intended to grant extraterritorial jurisdiction over individuals supporting terrorist organizations through the illicit drug trade. These statements by Senator Cornyn and Representative Hyde outlined Congress' concern about the relationship between the illegal narcotics trade and support of international terrorist organizations.[165] To combat this emerging dilemma, Congress enacted section 960a because they believed that section 960a would empower the United States to apprehend and try offending individuals in a U.S. court. Because both Los Zetas and the Juárez Cartel fulfill the criteria for FTO designation, the United States holds extraterritorial jurisdiction over members and affiliates of both DTOs who engage in the drug trade.

B. International Extradition Treaties

Though the Narcoterrorism Statute itself grants the United States jurisdiction over extraterritorial violations, a valid treaty of extradition must exist in order for the United States to compel a foreign perpetrator to appear in a U.S. court. According to the U.S. Attorney's Manual, the United States must submit a request for extradition via the Office of International Affairs pursuant to an existing extradition treaty between the United States and the relevant foreign nation.[166] Additional requirements may also apply if they exist within the extradition treaty itself, which both parties must follow during the extradition process.[167]

The extradition treaty relevant in this instance is the Extradition Treaty Between the United States of America and the United Mexican States ("Extradition Treaty").[168] Signed in 1978, the

---

[164] 151 CONG. REC. H6273, H6292 (daily ed. July 21, 2005) (statement of Rep. Hyde).
[165] 151 CONG. REC. S9846 (daily ed. Sept. 8, 2005 (statement of Sen. Cornyn); 151 CONG. REC. H6292 (daily ed. July 21, 2005) (statement of Rep. Hyde).
[166] DEP'T OF JUSTICE, U.S. ATTORNEY'S MANUAL, *supra* note 160.
[167] *Id.*
[168] *See generally* Treaty Signed at Mexico City, May 4, 1978 appd'x, Jan. 25, 1980, 31 U.S.T. 5059.

Extradition Treaty allows either nation to request the extradition of an individual accused of committing murder, fraud, rape, robbery, embezzlement, extortion, trafficking and cultivating illegal narcotics, and offenses relating to the international transit of goods.[169] Under this treaty, both nations are compelled to comply with an extradition request if the requesting nation's "laws would provide for the punishment of such an offense committed in similar circumstances."[170] If Los Zetas and the Juárez Cartel become designated as FTOs, drug trafficking or cultivating drugs for either cartel would violate section 960a. Therefore, Mexico must extradite these individuals to the United States upon request.[171]

VI. CONCLUSION

In 2012, several members of Congress attempted to pass a law designating Los Zetas, the Sinaloa Cartel, and the Gulf Cartel as terrorist organizations under the Immigration and Nationality Act.[172] This legislation ultimately died in the House of Representatives, and none of these cartels became FTOs.[173] This bill failed to distinguish between cartels engaging in acts reminiscent of traditional organized crime as opposed to those engaging in terrorism. Mexican drug cartels are traditionally known to commit acts of violence against opposing cartel members and those law enforcement members who pose major threats to drug operations. These DTOs are motivated by money when committing violence and do not seek to control vast areas of Mexican territory to create quasi-governmental structures.

---

[169] *Id.* (the Treaty includes various other criminal offenses, but the offenses listed pertain to Los Zetas and the Juárez Cartel).
[170] Treaty Signed at Mexico City, May 4, 1978 art. 1, Jan. 25, 1980, 31 U.S.T. 5059.
[171] To successfully extradite these individuals to the U.S., other treaty obligations must be followed, like presenting evidence and fulfilling timing requirements. *See generally* Treaty Signed at Mexico City, May 4, 1978 arts. 3, 4, 7, 8, 10, 12, and 13, Jan. 25, 1980, 31 U.S.T. 5059.
[172] This bill also included the Arellano Feliz Organization, the Beltran Leyva Organization, and La Família Michoacana. H.R. 4303, 112th Cong. (2012).
[173] *Bill & Summary Status, 112th Congress (2011-2012): H.R. 4303 All Congressional Actions*, THE LIBR. OF CONGRESS, THOMAS, http://thomas.loc.gov/cgi-bin/bdquery/z?d112:HR04303:@@@X (last visited Sept. 17, 2015) (showing the last major action taken in the House on this bill occurred on May 7, 2012).

Los Zetas and the Juárez Cartel, however, are not stereotypical cartels and thus should be designated as FTOs. These organizations create mayhem by indiscriminately attacking and killing Mexican civilians and migrants and significantly disturbing political life in Mexico and the United States. Both groups utilize terrorist tactics, like car bombings and beheadings, to further their goals of control, intimidation, and persuasion. Both are also not motivated only by monetary gain, for their actions ultimately lead to the disruption of the Mexican and American governments in significant ways.[174] Los Zetas in particular may be in the process of forming a relationship with Hezbollah or its affiliates.

In light of President Obama's Immigration Accountability Executive Action, the United States may experience an increase in illegal immigration along its southern border.[175] As a result, American national security likely faces increased violence, human trafficking, and death along regions of the U.S.-Mexico border controlled by Los Zetas and the Juárez Cartel.[176] Cartels target immigrants seeking to enter the United States illegally in order to use them to smuggle drugs[177] or to sell them into sex slavery.[178] Cartels like Los Zetas and

---

[174] *See, e.g.*, Press Release, Dep't of Justice, *supra* note 53; Chertoff, *supra* note 140, at 685.

[175] The Executive Action arguably creates an added incentive to enter the U.S. illegally in order to take advantage of the expanded "provisional waiver" and "Lawful Permanent Residents" statuses either immediately or at some point in the future. *See generally* Fact Sheet, The White House, Immigration Accountability Executive Action (Nov. 20, 2014), http://www.whitehouse.gov/the-press-office/2014/11/20/fact-sheet-immigration-accountability-executive-action; Ian Smith, *Yes, Amnesty Encourages More Illegal Immigration*, NAT'L REVIEW, Feb. 26, 2015, http://www.nationalreview.com/article/414436/ defying-common-sense-immigration-ian-smith (arguing that executive actions created by President Obama, including the creation of the Deferred Action for Childhood Arrivals program, incentivize migrants to cross the U.S.-Mexico border illegally).

[176] *See, e.g.*, Seper, *supra* note 41; *Juarez Cartel*, INSIGHT CRIME, http://www.insightcrime.org/mexico-organized-crime-news/juarez-cartel-profile (last visited Sept. 26, 2015).

[177] *See* Jess Rollins, *In Missouri, Illegal Immigrants Used to Smuggle Drugs*, USA TODAY (Feb. 10, 2013), http://www.usatoday.com/story/news/nation/2013/02/10/missouri-meth-smuggling-illegal-immigrants/ 1907003/.

[178] *See, e.g.*, Anne-Marie O'Connor, *Mexican Cartels Move into Human Trafficking*, THE WASH. POST (July 27, 2011), http://www.washingtonpost.com/world/americas/

the Juárez Cartel will likely take advantage of any influx in illegal immigration across the U.S.-Mexico border, posing a major threat to U.S. national security. The United States must implement a new policy to protect Americans and their interests against all current and future threats posed by cartels, especially those utilizing terrorist tactics.

The importance of designating both of these cartels as FTOs under section 219 of the Immigration and Nationality Act is crucial if the United States seeks to counter cartel violence. This designation refutes any notion that applying the Narcoterrorism Statute to individuals assisting designated cartels is improper. With the continuing threat of narcoterrorism adjacent to the American border, the potential for violence entering the United States is high. This is particularly true because both Los Zetas and the Juárez Cartel repeatedly target American civilians, police, and diplomats. To combat this major threat to national security, the United States must utilize current existing laws pragmatically and create a policy that does not repeat similar mistakes made in the recent past.

In the short term, a policy of tactical and relentless extraditions is an effective tool to combat terrorist funding in Mexico. The United States must not utilize extraditions of key terrorist leaders in the same manner used in Iraq and Colombia. The policy of "decapitation" of terrorist organizations continues to prove unsuccessful and, in the long term, detrimental to the security of American assets at home and abroad.[179] To better serve American interests, the U.S. government should seek to extradite individuals in the mid to lower ranks of these cartels as well as those individuals seeking to assist cartels in drug trafficking and cultivation. Section 960a should serve as both a way to incarcerate individuals that pose a major threat to American national security as well as dissuade those who aim to assist or are considering assistance as an option.

mexican-cartels-move-into-human-trafficking/2011/07/22/ gIQArmPVcI_ story.html.

[179] *See, e.g.*, Felbab-Brown, *supra* note 20, at 8.

COMMENT

CYBERSPACE:
THE 21ST-CENTURY BATTLEFIELD EXPOSING SOLDIERS, SAILORS, AIRMEN, AND MARINES TO POTENTIAL CIVIL LIABILITIES

Molly Picard*

In 2015, more than 25 million Americans were affected by the Office of Personnel Management data breaches. These incidents demonstrate a new form of warfare in an emerging battlefield that the United States must defend against: cyber warfare in cyberspace. And as part of that defense in the cyberspace battlefield, the U.S. Department of Defense and U.S. military are active members.

Among the various statutes governing the conduct of U.S. entities in cyberspace is the Computer Fraud and Abuse Act. Originally enacted in 1984 as part of the Comprehensive Crime Control Act, the Computer Fraud and Abuse Act was the U.S. Government's first attempt to legislate in the cyber security field and was designed to combat computer crimes, to secure government information, government computers, and government networks. Now, more than 30 years and several amendments later, the Computer Fraud and Abuse Act has expanded to cover nearly every

* George Mason University School of Law, Juris Doctor Candidate, December 2016; James Madison University, B.S. in Intelligence Analysis, magnum cum laude, 2013. I would like to thank CAPT Patrick Gibbons, U.S. Navy, Judge Advocate General Corps, for inspiring the topic of my comment, as well as CDR Paul Walker, U.S. Navy, Judge Advocate General Corps, for answering my questions and reviewing my comment. I would like to thank my notes editor, Lauren Doney, for providing insightful and timely feedback throughout the entire process of writing my comment. And, finally, I would like to thank my family and friends for their constant support.

computer in the world and makes illegal many activities that the average computer user undertakes on a regular basis.

Although the Computer Fraud and Abuse Act contains an exception for the lawful activities of law enforcement and U.S. intelligence agencies, the U.S. military is not a party to the exception. As the cyber security threat to the United States increases and the U.S. military's role in cyberspace evolves, the Computer Fraud and Abuse Act may expose members of the U.S. military active in U.S. cyber defense to personal, civil liabilities for acting in accordance with their orders. To avoid this unfortunate consequence, the Computer Fraud and Abuse Act must be revised and the U.S. military's role in cyber space must be better defined.

INTRODUCTION

> *At one minute out, the Black Hawk crew chief slid the door open. I could just make him out—his night vision goggles covering his eyes—holding up one finger. I glanced around and saw my SEAL teammates calmly passing the sign throughout the helicopter…*
>
> *An hour and a half before, we'd boarded our two MH-60 Black Hawks and lifted off into a moonless night. It was only a short flight from our base in Jalabad, Afghanistan, to the border with Pakistan, and from there another hour to the target we had been studying on satellite images for weeks…*
>
> *Crowded into the cabin around me and in the second helicopter were twenty-three of my teammates from the Naval Special Warfare Development Group…"Five minutes ago, the whole cabin had come alive. We pulled on our helmets and checked our radios and then made one final check of our weapons. I was wearing sixty pounds of gear, each gram meticulously chosen for a specific purpose, my load refined and calibrated over a dozen years and hundreds of similar missions…*
>
> *Now, as the Black Hawk flew to our target, I thought back over the last ten years….A decade after [the 9/11 attacks] and with eight years of chasing and killing al Qaeda's leaders, we were minutes away from fast-roping into Bin Laden's compound.*[1]

A personal account such as this is what most people expect when they think of Soldiers, Sailors, Airmen, and Marines—members of the United States' ("U.S.") armed forces—fighting the nation's enemies and providing for the nation's security. In the 21st-century, however, the nation's enemies have evolved. While members of the armed forces still engage in traditional combat described above, a new battlefield is emerging where engaging the enemy involves new weaponry—a mouse, a keyboard, and a computer—and in a new arena—cyberspace.[2] With this new

[1] MARK OWEN WITH KEVIN MAURER, NO EASY DAY: THE FIRST HAND ACCOUNT OF THE MISSION THAT KILLED OSAMA BIN LADEN 1-4 (2012).

[2] Cyberspace is defined by the Department of Defense as "[A] global domain within

battlefield come new challenges to the legal framework governing the conduct of the members of the U.S. armed forces in securing the nation from enemies, both foreign and domestic.

In fulfilling their mission to "support and defend the Constitution of the United States of America," the U.S. military regularly ask their members to conduct activities that would otherwise violate federal statutes and criminal codes.[3] For example, "[i]n wartime the role of the military includes the legalized killing (as opposed to murder) of the enemy . . . ."[4] The Computer Fraud and Abuse Act ("CFAA") has become an over-encompassing statute that now covers nearly every computer in the world.[5] Without creating an exception to the CFAA, members of the military could personally face civil liabilities for conducting operations in accordance with military orders. The Department of Defense's ("DOD") presence in cyberspace has increased in the past few years. This change became apparent with the recent establishment of United States Cyber Command ("CYBERCOM"), an entity designed to lead the military

---

the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." JOINT CHIEFS OF STAFF, JOINT PUB. 3-12(R): CYBERSPACE OPERATIONS, at GL-4 (Feb. 5, 2013) [hereinafter JP 3-12], http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

[3] *See* Enlistment Oath: who may administer, 10 U.S.C. § 502 (2006). *See also* U.S. CONST. art. 1, § 8, cl. 11 (Congress holds the power "[t]o declare War, grant Letter of Marque and Reprisal, and make Rules concerning Captures on Land and Water . . ."); U.S. CONST. art. 2, §1, cl. 1 ("The executive Power shall be vested in a President of the United States of America"); U.S. CONST. art. 2, § 2, cl. 1 ("The President shall be Commander in Chief of the Army and Navy of the United States…"); U.N. Charter, art. 51 (recognizing every nation's right to self-defense). *See e.g.*, MICHAEL WALZER, JUST AND UNJUST WARS: A MORAL ARGUMENT WITH HISTORICAL ILLUSTRATIONS 21-25 (Basic Books 5th ed. 2015) (providing reasons as to when certain conflicts are determined to be just or unjust).

[4] STEPHEN DYCUS ET AL., NATIONAL SECURITY LAW 404 (Aspen Casebook Series, Wolters Kluwer, 5th ed. 2011) (quoting Memorandum of Law: Executive Order 12333 and Assassination, by W. Hays Parks, *reprinted in* U.S. DEP'T OF ARMY, PAM. 27-50-204, THE ARMY LAWYER para. c. (Dec. 1989)).

[5] Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1561 (2010).

in the cyber security field.[6] Given the increasing cyber threat that puts industry, intellectual property, and national security at risk, it is important to define the military's role in this emerging cyberspace battlefield to avoid imposing civil liabilities on members of the armed forces who are merely following orders and upholding their mission to support and defend the United States.

The CFAA currently exempts law enforcement and intelligence agencies, enabling them to conduct activities that would otherwise violate the CFAA.[7] Those members of the military assigned to and operating under the authority of an intelligence agency, such as the Defense Intelligence Agency, National Security Agency, or Central Intelligence Agency, are privy to this exemption.[8] In contrast, however, members of the armed forces operating solely under military authority have no such protection. Instead, the military is required to justify each independent cyber operation.[9] Continuing to protect members of the armed forces from civil liabilities, which is done regularly when the United States sends its troops into battle, is essential to the success of CYBERCOM and for regulating the new cyberspace battlefield.

The current statutory framework surrounding cyber security law potentially exposes military personnel operating solely under military authority to civil liabilities for violating domestic laws, primarily the CFAA. To curtail the potential civil liabilities, the CFAA requires an amendment to create an exception for military cyber activities, similar to the exception granted to law enforcement operations and intelligences agencies. Additionally, the CFAA demands a reversion to its original intent of protecting government computer systems and sensitive government information. Finally, because of the indefiniteness surrounding cyberspace, the emerging

---

[6] *U.S. Cyber Command*, U.S. STRATEGIC COMMAND, https://www.stratcom.mil/factsheets/2/Cyber_Command/ (last updated Mar. 2015).

[7] Computer Fraud Abuse Act, 18 U.S.C. § 1030(f) (2008).

[8] *See id.* (§ 1030(f) specifically grants "an intelligence agency of the United States" the ability to conduct "any lawfully authorized . . . intelligence activity.").

[9] *See*, *e.g.*, Richard Weitz, *Defense Department Prepares for Cyberwar: The Current State of Play*, SECOND LINE OF DEF. (Apr. 12, 2011), http://www.sldinfo.com/ defense-department-prepares-for-cyberwar/.

21st-century battlefield warrants a clear statutory framework outlining the military's and DOD's roles in cyber security.

Section I of this comment introduces the current operating environment ("OE") by examining 21st-century national security threats to the United States. In explaining the OE, this comment then defines cyber security and explains the various types of cyberspace activities and cyber security threats. It discusses the military's emerging role in cyberspace and the activities the military conducts in cyberspace.

Section II describes the legal implications of cyber security and cyber operations by examining the international and domestic laws that establish the legal framework governing offensive and defensive cyber security missions.

Section III explains how current U.S. domestic law may expose members of the military to civil liabilities for conducting operations in accordance with military orders because of the overly broad scope of the CFAA and the lack of a clearly defined OE for the military in cyberspace. This analysis begins by examining *Nardone v. United States*. In *Nardone*, the Supreme Court held that a generally applicable statute that did not exempt the government or government agents from liability under the Federal Communications Act of 1934 prohibited the Bureau of Investigations from collecting data that the Federal Communications Act protected.[10] Using this case as well as traditional modes of statutory interpretation, this comment argues that the CFAA does not create an exception for military cyber activities, and because of this, members of the armed forces could potentially face civil liabilities for the military's cyber security activities. Although the CFAA creates exceptions for intelligence agencies and law enforcement operations, similar military actions are not included in the statute's exemption.

Finally, this comment suggests, in Section IV, that given the growing concern over cyber security and the ever-increasing threat to national security from cyberspace, the CFAA should be amended

[10] Nardone v. United States, 302 U.S. 379, 384-85 (1937).

to create an exception for military operations. Additionally, the CFAA should be reverted to its original intent of protecting government computer systems and sensitive government information. Finally, given the present cyber threat and growing cyber field, the military requires a general legislative framework to define the military's role in cyber operations so that the military can proactively address this new, emerging threat.

I. BACKGROUND: SETTING THE SCENE

A. The World Today

According to the May 2010, National Security Strategy ("NSS"), "[a]t the dawn of the 21st century, the United States of America faces a broad and complex array of challenges to [U.S.] national security."[11] In explaining the evolution of the world environment since the end of the Cold War, the NSS enumerates and advances persistent problems the United States has faced.[12] Specifically,

> [t]he circle of peaceful democracies has expanded; the specter of nuclear war has lifted; major powers are at peace; the global economy has grown; commerce has stitched the fate of nations together; and more individuals can determine their own destiny. Yet these advances have been accompanied by persistent problems. Wars over ideology have given way to wars over religious, ethnic, and tribal identity; nuclear dangers have proliferated; inequality and economic instability have intensified; damage to our environment, food insecurity, and dangers to public health are increasingly shared; and the same tools that empower individuals to build enable them to destroy.[13]

Following the terrorist attacks of September 11, 2001, the United States was forced to recognize the global threat of violent

[11] Press Release, The White House, Office of the Press Secretary, Fact Sheet: Nat'l Sec. Strategy 1 (May 2010) [hereinafter Nat'l Sec. Strategy Fact Sheet], http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.
[12] *Id.*
[13] *Id.*

extremist groups that continue to present a risk to U.S. national security.[14] Moreover, "[g]lobal power is becoming more diffuse," with new alliances emerging and power shifting throughout other regions of the world.[15]

The Worldwide Threat Assessment of the U.S. Intelligence Community lists counterintelligence, proliferation of weapons of mass destruction, terrorism, transnational organized crime, counterspace, and mass atrocities as major concerns to U.S. national security.[16] Competition over scarce resources also presents grave risks of instability.[17] Additionally, advances in technology accompanied by an increasing reliance on such technology continue to challenge the defense of the United States.[18] With this technology problem, there comes an increasing cyber security threat, which has become one of the gravest concerns to U.S. national security.[19]

B. Cyberspace: Understanding the 21st-Century Battlefield

As Congressman Jim Sensenbrenner explains, "[t]he United States has been the subject of the most coordinated and sustained computer attacks the world has ever seen."[20] Both the U.S. Government (USG) and America's private sector are regularly victims of "military style hacks."[21] Responding to such attacks

---

[14] OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, THE NATIONAL INTELLIGENCE STRATEGY OF THE UNITED STATES OF AMERICA 4 (2014) [hereinafter NATIONAL INTELLIGENCE STRATEGY], http://www.dni.gov/files/documents/2014_ NIS.pdf.
[15] *Id.*
[16] *Annual Open Hearing on Current and Projected National Security Threats to the United States: Hearing Before the S. Select Comm. on Intelligence*, 113th Cong. 10 (2013) (statement for the record of James R. Clapper, Director of National Intelligence) [hereinafter *Worldwide Threat Assessment*], http://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pd.
[17] NATIONAL INTELLIGENCE STRATEGY, *supra* note 14, at 4.
[18] *Id.*
[19] *Worldwide Threat Assessment*, *supra* note 16, at 12.
[20] *Investigating and Prosecuting 21st Century Cyber Threats*: *Hearing Before the Subcomm. on Crime, Terrorism, Homeland Security and Investigations of the H. Comm. on the Judiciary*, 113th Cong. 1 (2013) (statement of Rep. F. James Sensenbrenner, Chairman, H. Subcomm. on Crime, Terrorism, Homeland Security and Investigations) [hereinafter Statement of Senator Sensenbrenner].
[21] *Id.* at 2.

requires more than international diplomacy as they present serious challenges to America's national security as well as its businesses and economy.[22] Given the increasing global reliance on computer related technologies, as evident by the more than two billion internet users in 2010, cyber security concerns will continue to increase in number and severity.[23]

The first step to understanding cyber security is understanding the emerging battlefield that is becoming a part of everyday life—that is, understanding the meaning of "cyberspace." The USG defines cyberspace "as the global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[24] Because of the world's increasing reliance on cyber technologies, "[c]yberspace [has become]…a key sector of the global economy [and] has become an incubator for new forms of entrepreneurship, advances in technology, the spread of free speech, and new social networks that drive [economies]." [25] Moreover, the United States' key infrastructure industries—"including [the] energy [sector], banking and finance, transportation, communication, and the Defense Industrial Base"—are becoming increasingly reliant on cyber technologies.[26] This increases the risks to the United States as the systems that these industries rely on "may be vulnerable to disruption or exploitation" by enemies of the United States.[27] Unfortunately, while the United States increases its reliance

---

[22] *Id.*

[23] DEP'T OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 1 (2011), [hereinafter DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE], http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/DOD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf.

[24] Andru E. Wall, *Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action*, 3 HARV. NAT'L SEC. J. 85, 117 (2011-2012) (quoting JOINT PUB. 1-02, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 95 (2011)).

[25] DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE, *supra* note 23, at 1.

[26] *Id.*

[27] *Id.*

on cyberspace, cyber defense and security have not grown at the same rate.[28]

The concept behind "cyberspace" and its continued operation today, was to increase connectivity and the ability to share information quickly. Advances in cyber technology have made it so that "[s]mall-scale technologies can have an impact disproportionate to their size; potential adversaries do not have to build expensive weapons systems to pose a significant threat to [the United States'] national security."[29] This potentially means that an individual or a handful of individuals working together can cause huge impacts with a small amount of resources. While the United States successfully defends against a multitude of cyberattacks and intrusions on a daily basis, the cyber field and creative enemies and criminals are designing new technologies at an alarming rate that may outpace U.S. defensive capabilities.[30]

C. Cyber Warfare: Understanding Cyber Attacks

Cyber attacks come in a variety of shapes and forms. Possible scenarios range from "a virus that scrambles financial records or incapacitates the stock market, to a false message that causes a nuclear reactor to shut off or a dam to open, to a blackout of the air traffic control system that results in airplane crashes."[31] All of these scenarios have the potential to cause "severe and widespread economic or physical damage."[32] The resulting damage lies on a spectrum from "merely annoying to destructive," and may aim to "facilitate future criminal, espionage or military activities."[33] Cyber operations may be designed merely to gather information or gain access to a system, or they "can go much further…adversely affecting the functionality of a computer system or even destroying a system

[28] *Id.*
[29] *Id.* at 2.
[30] *Id.*
[31] Oona A. Hathaway et al., *The Law of Cyber-Attack* 100 CAL. L. REV. 817, 822-23 (2012) (internal citations omitted).
[32] *Id.* at 823.
[33] Gary D. Brown & Owen W. Tullos, *On the Spectrum of Cyberspace Operations*, SMALL WARS JOURNAL (Dec. 11 2012), http://smallwarsjournal.com/print/13595.

or component."[34] Some broad categories of attacks include access operations, disruption operations, and cyber attacks.[35]

"Access operations enable other cyber activities by providing entry to an adversary computer system," which is necessary before any other cyber activity, such as information gathering or attacks, can take place.[36] An attacker may gain access to computers or information systems "by installing software programs, defeating security measures, injecting malicious code or other exploitation of a system's vulnerabilities," and include actions to maintain or regain access previously obtained.[37]

In 2008, an access attack occurred when Operation Buckshot Yankee used universal serial buses ("USB") programmed with a virus to gain access to sensitive information.[38] When a user inserted the USB into a port on a classified DOD network computer connected to the Internet, the actors were able to gain access to information on the networks being used by the computer. "Operations like this can be designed to facilitate espionage or the destruction of a system, or anything in between."[39]

A second example, Operation Aurora "gained and maintained access into Google's network for many months," which gave the actors, "a treasure trove of information [on] companies that were doing business with Google."[40] The attack permitted access to a large quantity of information, and was believed to have originated in China for purposes of industrial espionage.[41]

And in 2009, operation GhostNet was able to "turn on an infected computer's microphone and video recording systems [ ] to

---

[34] *Id.*
[35] The following examples were excerpted from *On the Spectrum of Cyberspace Operations*, by Gary D. Brown & Owen W. Tullos. *See id.*
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] Brown & Tullos, *supra* note 33.
[40] *Id.*
[41] *Id.*

capture new information, or [ ] to exfiltrate data from the computer system."[42] Believed to have originated in China, the attack gained unauthorized access to computer systems in over 100 countries.[43]

Another type of operation is a cyber attack, which may be defined as an activity that "has effects in the real world beyond the cyber system itself" such as "actions in cyberspace whose foreseeable results include damage or destruction of property, or death or injury to persons."[44] In 2009, the Sayano-Shushenskaya Russian hydroelectric power plant suffered a serious accident. Workers shut down a dam's damaged turbine for maintenance; but a computer operator located at a separate control facility from the dam turned the turbine back on.[45] "The operator's electronically delivered command for increased activity caused the damaged turbine to spin out of control, killing 75 people and causing over $1 billion damage."[46] While this was an accident, it demonstrates the potential damage to infrastructure if individuals seeking to cause harm gained access to critical infrastructure computer systems.[47]

Cyber disruptions are a third type of cyber operations that "interrupt the flow of information or the function of information systems without causing physical damage or injury."[48] Cyber disruptions can interfere with a government's ability to communicate with its people or can include the distribution of false information through an "official electronic message system" that advocates for actions to be taken against the target government.[49] An excellent example of a cyber disruption is the 2010 incident named Operation Cupcake. Al Qaeda in the Arabian Peninsula ("AQAP") published

[42] *Id.*
[43] *Id.*
[44] *Id.* (noting that this definition differs from DOD's, which will be explained in the following section).
[45] Brown & Tullos, *supra* note 33.
[46] *Id.* (noting that this definition differs from DOD's, which will be explained in the following section).
[47] *Id.*
[48] *Id.*
[49] *Id.*

an online version of the magazine *Inspire*.[50] "[T]he British government replaced the bomb-making instructions in the online publication with cupcake recipes," which lasted for several days.[51]

Another example of a cyber disruption occurred on July 4, 2009. Both the United States and South Korea suffered an attempt to "jam traffic on over two dozen government and commercial systems, including financial networks."[52] While the effects lasted only hours to a few days, such an attack could be replicated and cause further, lasting impacts.[53]

A third example occurred in 2007, when "[c]yber actions [in Estonia] shut down the Government's ability to communicate and froze the financial sector for about a month."[54] The attackers were motivated by a civil dispute—the Estonian government wanted to move the statue of a Soviet soldier and the perpetrators disagreed with this decision.[55] "Estonia heavily relied on cyberspace for communications and commerce, and experienced significant disruption of its communication and economic systems."[56]

And, finally, when Russia invaded Georgia in 2008, the nation simultaneously launched traditional military attacks and a cyber offensive. Georgia's web and telecommunications systems suffered a cyber disruption that prevented "many government computer-based activities in the early days of the Russo-Georgian conflict."[57] Georgia's civilian communications, financial systems, and media were also degraded by the cyber operations.[58]

---

[50] *See id.*
[51] Brown & Tullos, *supra* note 33.
[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] *Id.*
[56] *Id.*
[57] Brown & Tullos, *supra* note 33.
[58] *Id.*

As these examples suggest, "[c]yberwarfare is no longer the future of warfare—it is the present and the future."[59] Currently cyberspace is filled with "minor skirmishes, a silent cyber arms race, and major intelligence gathering."[60] These small, precursory actions may be setting the stage for larger cyber wars in the future; early stages of cyber activity demonstrates that countries are eager to learn as much as possible about U.S. critical infrastructure and information systems.[61]

In 2015, the U.S. Office of Personnel Management ("OPM") suffered two separate, but related cyber security incidents that resulted in the disclosure of personnel data of 4.2 million current and former federal government employees and the background investigation records of 21.5 million current, former, and prospective federal employees and contractors.[62] OPM discovered malicious activity on the OPM network, which permitted the source of the incidents to steal information from the OPM-maintained background investigation databases.[63] The USG has yet to reveal the source of these cyber security incidents, and OPM, the Department of Homeland Security ("DHS"), and the Federal Bureau of Investigation ("FBI") continue to investigate, assess the full impact, and assist with the remedial efforts following the incidents.[64] Although this collaborative team assessed that the attack is no longer active, the USG has not stated how the source gained access or for how long the attack went undetected.[65] This massive data breach demonstrates the potential impact of an access attack and highlights the pertinence of cyber security to the United States.

---

[59] Wall, *supra* note 25, at 115.
[60] *Id.*
[61] *Id.*
[62] OFFICE OF PERS. MGMT., CYBERSECURITY RESOURCE CENTER: CYBERSECURITY INCIDENTS (last visited Nov. 06, 2015) https://www.opm.gov/cybersecurity/cybersecurity-incidents/#WhatHappened.
[63] OFFICE OF PERS. MGMT., CYBERSECURITY RESOURCE CENTER: FREQUENTLY ASKED QUESTIONS (last visited Nov. 06, 2015) https://www.opm.gov/cybersecurity/faqs.
[64] *Id.*
[65] *Id.*

D. United States Cyber Command

In response to the growing threat of cyber warfare and the growing concern over cyber security, the DOD established U.S. Cyber Command ("CYBERCOM"). CYBERCOM is a sub-unified command nestled under the control of U.S. Strategic Command ("STRATCOM"). CYBERCOM is a topic-focused command, which joined other Combatant Commands ("COCOMs") such as U.S. Central Command ("CENTCOM"), U.S. Special Operations Command ("SOCOM"), and U.S. Africa Command ("AFRICOM"). COCOMs become the lead for the military and focus specifically on their respective topic or geographical areas. CYBERCOM's mission is to:

> Plan[], coordinate[], integrate[], synchronize[] and conduct[] activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to [the U.S.] adversaries.[66]

This mission is broad and grants CYBERCOM wide authority to take both defensive and offensive actions in cyberspace.[67] More specifically, DOD has identified three focus areas for CYBERCOM: "[d]efending the DODIN [Department of Defense Information Network], providing support to combatant commanders for execution of their missions around the world, and strengthening [the U.S.'s] ability to withstand and respond to cyber attack[s]."[68] CYBERCOM intends to improve "DOD's capabilities to operate resilient, reliable information and communication networks, counter cyberspace threats, and assure access to cyberspace."[69]

---

[66] *U.S. Cyber Command*, U.S. STRATEGIC COMMAND (last updated Mar. 2015), http://www.stratcom.mil/factsheets/2/Cyber_Command/.
[67] *See id.*
[68] *Id.*
[69] *Id.*

Furthermore, DOD has identified five key strategic initiatives for CYBERCOM to accomplish. The strategic initiatives are as follows:

> (1) DOD will treat cyberspace as an operational domain to organize, train, and equip so that DOD can take full advantage of cyberspace's potential; (2) DOD will employ new defense operating concepts to protect DOD networks and systems; (3) "DOD will partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy; (4) DOD will build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity; and (5) DOD will leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.[70]

Thus, through CYBERCOM, DOD aims to improve training, education, and techniques, as well as establish partnerships with the private sector and international partners in order to meet the cyber security demands of cyberspace.

DOD is increasing its focus on cyberspace and exploring strategic objectives that will enable it to encounter 21st-century threats. DOD recognizes that "[d]evelopments in cyberspace provide the means for the US military, its allies, and partner nations to gain and maintain a strategic, continuing advantage in the OE, and can be leveraged to ensure the nation's economic and physical security."[71] Because cyberspace has created a paradox where both the "prosperity and security" of the United States "have been significantly enhanced" by cyberspace, yet cyberspace has "led to increased vulnerabilities and a critical dependence on cyberspace," [72] DOD, through CYBERCOM, is attempting to synchronize offensive and defensive measures in cyberspace in support and defense of the United States.

---

[70] DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE, *supra* note 23, at 10 (quoting the 2010 National Security Strategy).
[71] JP 3-12, *supra* note 2, at v.
[72] *Id.*

CYBERCOM operates under the authorities of the Secretary of Defense ("SECDEF") and integrates defensive and offensive operations by synchronizing the activities of the COCOMs, Joint Staff, Office of the Secretary of Defense, the individual military branches, other government departments, and agencies.[73] DOD must conduct cyber operations in accordance with U.S. domestic law, applicable international law, relevant USG and DOD policies, and during times of armed conflict, DOD operations must follow the law of armed conflict by complying with the "fundamental principles of military necessity, unnecessary suffering, proportionality, and distinction."[74] Thus, it is crucial to understand the legal framework that governs cyberspace. Military cyber operations that may be in conflict with this framework present serious issues for the DOD.

II. THE CURRENT LEGAL FRAMEWORK IN CYBERSPACE

The law regulating cyberspace is neither clear nor precise. To understand the legal framework that governs cyberspace, and the actions that violate this framework, it is important to understand both international legal concepts and domestic laws. "While cyber operations must satisfy both international and domestic law, the elements of analysis differ. An action may be permissible under international law, but face domestic legal or policy restrictions."[75] While domestic law usually controls in U.S. courts, international legal principles often inform domestic law principles.[76] Section II is

[73] *Id*. at vii-x.

[74] *Id*.

[75] Brown & Tullos, *supra* note 33.

[76] *See* DYCUS ET AL., *supra* note 4, at 163. When at war, the U.S. is bound by the principles of *jus in bellum*, which governs conduct when at war. *See*, *e.g.*, Geneva Convention Relative to the Treatment of Prisoners of War art. 3, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135. The U.S. is bound by the Geneva Conventions and Hague Conventions as a signatory. *See generally* Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Convention (XI) relative to certain Restrictions with regard to the Exercise of the Right of Capture in Naval War, Preamble, Oct. 18, 1907, 36 Stat 2396. Furthermore, the United States is bound by the concept of *jus ad bellum*, which limits when a nation may engage in war. This concept is largely inferred from the U.N. Charter, which stipulates when a nation may use military force. *See generally* U.N. Charter,

divided into three parts. Part A explains how customary international law generally applies to cyberspace. Part B outlines the domestic legal framework. Finally, Part C describes CFAA in detail and examines the potential civil liabilities that could arise under the statute against members of the armed forces. CFAA is a domestic policy of particular concern for the DOD.

A. Traditional International Law

The end of World War II brought a wave of international treaties attempting to define permissible uses of force and the laws governing conduct when nations are at war.[77] The international community was largely concerned with establishing and maintaining peace, and limiting the use of force to situations where it was the only means capable of resolving disputes and reinstating international peace and security.[78] One area in which these international agreements have become inadequate is in determining "how to address attacks that have little or no direct physical consequences, but that nonetheless cause real harm to national security," such as attacks in cyberspace.[79] While nation states have fallen short of claiming that a cyber attack would give rise to the requisite armed attack necessary for justifying a response using military force under Article 51 of the United Nations ("U.N.") Charter, there is a general

arts. 42, 43, and 51. Together, these international concepts shape how and when the U.S. engages in war. The U.S. is bound by these concepts based on treaties and signed international agreements. However, if Congress creates statutes contrary to these concepts, then the U.S. statutes rule under the "last in time" principle. *See* Comm. of U.S. Citizens Living in Nicaragua v. Reagan, 859 F.2d 929, 929 (1988). Furthermore, the U.S. does not believe itself to be regulated by customary international law or by international concepts that have not been adapted into U.S. statutes or made law through the treaty process. *Id*. at 936. Thus, while the United States' policies toward engaging in war and the United States' conduct once in war have been shaped by international law, the United States' places what has been codified in treaties and statutes above international law.

[77] *See* Hathaway, *supra* note 31, at 840 (referencing the Geneva Conventions and the U.N. Charter).

[78] *See* DYCUS ET AL., *supra* note 4, at 210-12 (explaining that even when use of force is permissible, it must be limited only to effectuate legitimate political goals).

[79] Hathaway, *supra* note 31, at 840.

consensus that cyber attacks are an increasing threat to national and international peace and security.[80]

International legal concepts regarding the use of military force necessarily involve two concepts: *jus ad bellum,* or the international laws concerning a nation's right to wage war, and *jus in bello*, or the laws governing armed conflict once it has begun.[81] Understanding how these concepts relate to cyber security first requires a basic understanding of these concepts and how cyber security concerns differ from the pre-computerized world that existed when these concepts were formed and codified in international treaties and agreements.

1. Jus ad bellum

Jus ad bellum incorporates the understanding expressed in the U.N. Charter for when nation states may go to war. Article 2 of the U.N. Charter states that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations" in order to preserve international peace and security.[82] The prohibition against the use of force has two general exceptions: member nations are permitted to use force when they are taking part of collective security operations and "[when use of force] actions [are] taken in self-defense."[83] Thus, the crux of the debate is whether a cyber attack is analogous to an armed attack, thus enabling a state to respond in self-defense.[84] Because not every offensive action taken by one party against another rises to the level of an armed attack, it is questionable as to whether cyber attacks may amount to the use of force required to trigger a permissible use of force in response.[85] Additionally, determining the degree or the severity of a cyber

[80] *See id*.
[81] DYCUS ET AL., *supra* note 4, at 211, 234.
[82] U.N. Charter, art. 2, para. 4.
[83] Hathaway, *supra* note 31, at 843-44 (outlining the exceptions to the authorization of use of force located in U.N. Charter Articles 39 and 51).
[84] *See* U.N. Charter art. 51. *See also* Hathaway, *supra* note 31, at 844.
[85] Hathaway, *supra* note 31, at 844-45.

attack's impact and whether it justifies taking reciprocal, defensive actions is no easy feat.[86]

Moreover, the United States has recognized that the international law principles of necessity and proportionality apply to cyber attack responses.[87] These principles limit the use of force, making responsive military actions a possibility only as a last resort when all diplomatic means have failed, and these principles require that an appropriate response be no more excessive in force than what is absolutely necessary to achieve legitimate political objectives.[88] The challenge again comes down to determining what is the appropriate degree of responsive action to a cyber incident and whether and at what point military force may be used in such a response.[89]

2. Jus in bello

When a state launches an armed attack, and the attack was sufficient to justify a response, the international law concept of *jus in bello* governs conduct during an armed conflict.[90] *Jus in bello* emphasizes four key principles that comprise an overarching guide to acceptable conduct in armed conflict: necessity, proportionality, distinction, and neutrality.[91] "Necessity relates to the concrete military advantage" that a military action attempts to gain, and if the actions do not advance the military's objective, they may be unnecessary and therefore prohibited.[92] Proportionality deals with the relation between the military advantage sought by the attack and the resulting harm caused to civilians; if the "incidental loss of civilian life, injury to civilians, damage to civilian objects, or a

[86] *See generally id.* at 845-49.
[87] *Id.* at 849.
[88] *See* DYCUS ET AL., *supra* note 4, at 234.
[89] *See* Hathaway, *supra* note 31, at 848-50.
[90] DYCUS ET AL., *supra* note 4, at 211, 234.
[91] *See* Hathaway, *supra* note 31, at 850-55.
[92] *Id.* at 850.

combination thereof," far exceeds the military advantage, the response may be inappropriate and prohibited.[93]

The principle of distinction restricts the victims of attacks to military targets, and places relatively strict limits on who can perpetrate and who can be the target of responsive actions.[94] Distinction in responding to or conducting cyber activities is an interesting consideration. Under international law, civilians are not supposed to be the intended targets of military actions; however, because enemies are no longer clearly defined and computer systems are intertwined, the principle of distinction presents a unique challenge for responding to cyber attacks.

Lastly, the concept of neutrality pertains to nation states that declare neutrality in a conflict. This declaration of neutrality, however, does not keep independent actors from using the information systems and networks of a neutral state to launch an attack.[95] Thus, the neutrality principle raises questions over how much control a nation state must maintain over its networks, especially if it is a neutral state, and who, then, becomes responsible for the use of the networks in a cyber attack launched from a neutral nation.[96]

While customary international law establishes a legal framework for traditional armed conflict, cyberspace challenges the concepts of *jus ad bellum* and *jus in bello*. The principles may very well be adaptable to cyberspace. However, finding the necessary armed attack that warrants a response using military force may prove more difficult in the context of cyber warfare. Further complicating the issue is the difficulty of defining an appropriate response to a cyber attack of sufficient magnitude while considering the four key principles governing armed conflict once it begins.

---

[93] *Id*.
[94] *Id*. at 851-52.
[95] *Id*. at 855.
[96] *Id*.

3. Countermeasures

The international concept of countermeasures provides more definitive guidance on responding to a cyber security incident. The principle states, "when a state commits an international law violation, an injured state may respond with a countermeasure."[97] Cyber attacks that may not rise to the level of an armed attack may still violate international customary law and may warrant an appropriate countermeasure.[98] Countermeasures, however, are intended only to coerce the state committing the act that is violating international law to cease its unlawful activities; and once the unlawful activities have stopped, the use of countermeasures must also stop.[99] For example, if a nation was hacking a government computer network in order to obtain information, the victim of the attack may be able to launch a counterattack; however, once the initial aggressor ceases the attack, the response must also cease. Additionally, if countermeasures must comply with the four key principles of *jus in bello*, appropriate responses may be rather limited and difficult to define.

4. International Law in the United States

Generally, the U.S. is bound by the concepts of *jus in bello* and *jus ad bellum* where these concepts have been incorporated into U.S. law through treaties, statutes, and the adoption of international agreements such as the Geneva Conventions, Hague Conventions, and U.N. Charter.[100] When, however, the United States creates a statute governing the same matter as an international agreement or treaty, the "last in time" principle governs, where a statute that supersedes an international agreement does away with the United States' responsibility to act in accordance with the superseded policy.[101] Furthermore, when the United States wishes to enter a conflict, the branches of the USG disagree on whether the President,

[97] Hathaway, *supra* note 31, at 857.
[98] *Id.*
[99] *Id.* at 857-58.
[100] DYCUS ET AL., *supra* note 4, at 234-35.
[101] *Id.* at 185-89.

acting under the Commander in Chief power alone and regardless of Congress's war powers or international agreements, may introduce the military into combat, for how long, and what actions the President can authorize. [102]

While international organizations such as the U.N. and North Atlantic Treaty Organization ("NATO") have discussed the need for cooperation in cyberspace, the international community only reached a mere general consensus declaring that more discussion is warranted for determining a legal standard for cyberspace.[103] Depending on the target or type of attack, aviation law, law governing outer space, and maritime law may provide further guidance on international legal concepts governing cyberspace.[104] Currently, however, international legal concepts provide nothing more than a collection of laws that may only apply under specific contexts. International legal principles were established well before the modern concept of cyber security was a concern, creating similar problems to those regarding the application of international law to conflicts involving terrorist organizations and other non-state actors.[105] While perhaps establishing a starting point, international law does not currently provide a legal standard for cyberspace. This is especially problematic given international law's control over armed conflict and the fact that most modern rules of war were adapted from customary principles of international law.

Thus, while some international legal concepts bind the United States, the applicability of international law is muddled by modern conflicts, including cyber security, where the international

[102] *Id.* at 267-75 (citing presidential use of the Commander in Chief power in entering Vietnam).
[103] Hathaway, *supra* note 31, at 860-64; *see also* OFFICE OF THE PRESS SEC'Y, THE WHITE HOUSE, PPD-21, PRESIDENTIAL POLICY DIRECTIVE – CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (2013), http://www.whitehouse.gov/ the-pressoffice/2013/ 02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (explaining that it is U.S. policy to cooperate with international partners on cyber security matters).
[104] Hathaway, *supra* note 31, at 868-73.
[105] *See* DYCUS ET AL., *supra* note 4, at 234-35.

law has not yet been developed, and the disagreements over engaging in conflict are unsettled.

B. Domestic Law

In *2001: A Space Odyssey*, H.A.L., an artificially intelligent computer takes over a space ship sent on an outer space mission to find extraterrestrial life.[106] At its debut in 1968, the idea that a computer might be able to manipulate and take control of a mission and then kill human beings likely seemed far-fetched and revolutionary. Rather than reality, this likely seemed like the wild dream of a science fiction fanatic. Yet, some 46 years later, the threat posed by cyberspace, or the "global domain within the information environment consisting of the interdependent network of information systems [107] infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers," is quickly approaching a risk level similar to that of H.A.L.[108] Rather than having a clearly defined statutory scheme for dealing with an increasingly complex cyber security environment, the current legal framework is a hodgepodge of more than 50 federal statutes, some dating back to the 1800's.[109] These statutes attempt to govern 10 broad themes that are particularly relevant to the cyber security interests of the U.S. and its citizens:

> national strategy and the role of government, reform of the Federal Information Security Management Act (FISMA), protection of critical infrastructure (especially the electricity grid and the chemical industry, information sharing and cross-sector coordination), breaches resulting in theft or exposure of personal data such as financial information, cybercrime offenses and penalties, privacy in the context of electronic

[106] *See* 2001: A SPACE ODYSSEY (Metro-Goldwyn-Mayer 1968).
[107] Where information systems are defined as "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." ERIC A. FISCHER, CONG. RESEARCH SERV., R42114 FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW AND DISCUSSION OF PROPOSED REVISIONS 1 (2013).
[108] *Id.*
[109] *Id.* at 1-2, 21, 52.

> commerce, international efforts, research and development (R&D), and the cybersecurity workforce.[110]

As cyberspace continues to present an increasing threat to the U.S., legislators have been grappling to resolve issues relating to the key themes of cyber security and the current legal framework governing cyberspace. To some extent, the White House, the Senate, and the House of Representatives have been unable to agree on which agency should lead the nation's cyber security; currently that responsibility rests with DHS, at least for the time being.[111] Rather than having a clearly defined, ascertainable standard for infrastructure protection, the White House has promulgated a regulatory framework aimed at ensuring the United States' critical infrastructure, with DHS in charge of regulating those safeguards.[112]

Moreover, the "size, skills, and preparation of the federal and private-sector cybersecurity workforce," has concerned national-level policy makers, who have attempted to address issues such as education and training through legislative efforts.[113] "The need for improvements in fundamental knowledge of cybersecurity and new solutions and approaches . . . [to address] topics such as detection of threats and intrusions, identity management . . . , and supply chain security," have been recognized in many recent legislative actions.[114] Without a cohesive approach to operational security, managing threats and ensuring that agencies comply with national standards presents serious challenges to those responsible for securing

---

[110] *Id.* at 4-5 (formatting omitted).

[111] *See id.* at 9-10. *See also* U.S. DEP'T OF HOMELAND SEC., BLUEPRINT FOR A SECURE CYBER FUTURE: THE CYBER SECURITY STRATEGY FOR THE HOMELAND SECURITY ENTERPRISE 2 (2011), http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf; PDD-21, *supra* note 103 (explaining that DHS is the lead on protection of critical infrastructure while the Department of Justice and the FBI take the lead on counterintelligence and counterterrorism efforts related to critical infrastructure).

[112] *See generally* THE WHITE HOUSE, REGULATORY FRAMEWORK FOR COVERED CRITICAL INFRASTRUCTURE 1-9, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cybersecurity-regulatory-framework-for-covered-critical-infrastructure-act.pdf.

[113] FISCHER, *supra* note 107, at 10.

[114] I*d.* at 11.

cyberspace.[115] Furthermore, legislating in the cyber world presents complex policy issues because there are close ties between federal and private sector cyber systems, especially related to private-sector-owned critical infrastructure and the information sharing environment.[116]

In this mix of authorities granting permission to various agencies and departments, there is a complex framework governing cyberspace.[117] Furthermore, with the potential number of players involved—DHS, DOD, Congress, the Intelligence Community, the private sector, just to name a few—managing the web of applicable authorities, statutes, and regulations is cumbersome. While recognizing that cyber security is a major concern for U.S. national security and the importance of protecting critical infrastructure, cyber security frameworks are complicated by the mass of federal statutes that may apply to cyberspace.[118] Further complicating the issue are statutes like the CFAA; a law designed to increase the U.S. cyber security, but one that may create liabilities for actions taken by U.S. military personnel.

C. The CFAA and Its Developments over the Years

The CFAA finds its origins in the Comprehensive Crime Control Act of 1984, which was Congress's first attempt to legislate for the emerging cyber threat.[119] The CFAA emerged in 1986 after Congress investigated problems associated with computer crimes and attempted to legislate the developing cyber security field.[120] It

[115] *See also id.* at 52-61 (including a table with federal statutes deemed by CRS to have cyber security provisions).
[116] *Id.* at 13-15.
[117] *See id.* (summarizing the federal statutory framework governing cyber security).
[118] *See generally* Nat'l Security Strategy Fact Sheet, *supra* note 12, at 2; NATIONAL INTELLIGENCE STRATEGY, *supra* note 14, at 4; *Worldwide Threat Assessment*, *supra* note 16, at 2.
[119] H. MARSHALL JARRETT, ET AL., COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION CRIMINAL DIVISION, PROSECUTING COMPUTER CRIMES 23 (2010).
[120] *See id.* at 1-3.

was designed to be "a tool for law enforcement to combat computer crimes."[121] In its current form, the CFAA

> outlaws conduct that victimizes computer systems. It is a cyber security law. It protects federal computers, bank computers, and computers connected to the Internet. It shields them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud. It is not a comprehensive provision, but instead it fills cracks and gaps in the protection afforded by other federal criminal laws.[122]

The legislative history indicates that Congress intended these provisions to provide "'a clearer statement of proscribed activity' to 'the law enforcement community, those who own and operate computers, as well as those who may be tempted to commit crimes by unauthorized access.'"[123]

Because of the way that the CFAA evolved throughout the years, a "statute… designed to criminalize only important federal interest computer crimes potentially regulates every use of every computer in the United States and even many millions of computers abroad."[124] The USA PATRIOT Act amended the CFAA's definition used to define target computers, or the computers that are targeted in order to obtain information or take further, harmful actions. The CFAA refers to such a target as a "protected computer," which it defines as "computers used in or affecting interstate or foreign commerce and computers used by the federal government and financial institutions."[125] Essentially, the definition is so expansive that in order to qualify as a "protected computer," "it is enough that the computer is connected to the Internet."[126] Additionally, the USA PATRIOT Act amendments further expanded the definition to

---

[121] Statement of Senator Sensenbrenner, *supra* note 21, at 2.
[122] CHARLES DOYLE, CONG. RESEARCH SERV., R 97-1025, CYBERCRIME: AN OVERVIEW OF THE FEDERAL COMPUTER FRAUD AND ABUSE STATUTE AND RELATED FEDERAL CRIMINAL LAWS (2010) (text excerpted from the Summary located before the table of contents).
[123] JARRETT ET AL., *supra* note 119, at 1.
[124] Orin S. Kerr, *supra* note 5, at 1561.
[125] DOYLE, *supra* note 122, at 47.
[126] *Id*. at 1.

include all computers inside or outside of the United States, "so long as they affect 'interstate or foreign commerce or communication of the United States.'"[127]

A broad overview of the CFAA can be established by summarizing the seven general subsections of 18 U.S.C. § 1030 (a) and sections (b)-(g) of the statute. Section 1030 (a)(1) outlaws accessing a computer to commit espionage against the United States.[128] Section 1030 (a)(2) "outlaws computer trespassing (e.g., hackers) resulting in exposure to certain governmental, credit, financial, or computer-housed information."[129] To violate section (a)(2), one must "(1) [i]ntentionally access a computer, (2) without or in excess of authorization, (3) [to] obtain information (4) from financial records of financial institution or consumer reporting agency, OR the U.S. government, OR a protected computer."[130] Section 1030 (a)(3) outlaws computer trespassing (hacking by outside users) into a government computer, even if no information is obtained.[131]

Section 1030 (a)(4) outlaws committing fraud, an integral part of which involves unauthorized access to a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce.[132] To demonstrate a violation under section (a)(4), one must "(1) [k]nowingly access a protected computer without or in excess of authorization, (2) with intent to defraud, (3) [where the] access furthered the intended fraud, and (4) obtained anything of value, including use if value exceeded $5000."[133] Section 1030 (a)(5) outlaws damaging a government computer, a

[127] JARRETT ET AL., *supra* note 119, at 5.
[128] *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (a)(1) (2008); DOYLE, *supra* note 122, at 1; JARRETT ET AL., *supra* note 119, at 12.
[129] *See* 18 U.S.C. § 1030(a)(2); DOYLE, *supra* note 122, at 2; JARRETT ET AL., *supra* note 119, at 16-17.
[130] JARRETT ET AL., *supra* note 119, at 16.
[131] *See* 18 U.S.C. § 1030(a)(3); DOYLE, *supra* note 122, at 2-3; JARRETT ET AL., *supra* note 119, at 23.
[132] *See* 18 U.S.C. § 1030(a)(4); DOYLE, *supra* note 122, at 46-48; JARRETT ET AL., *supra* note 119, at 26.
[133] JARRETT ET AL., *supra* note 119, at 26.

bank computer, or a computer used in, or affecting, interstate or foreign commerce (*e.g.*, using a worm, computer virus, Trojan horse, time bomb, a denial of service attack, or other forms of cyber attack, cyber crime, or cyber terrorism).[134] Section (a)(5) has three subsections. To implicate section (a)(5)(A), one must "(1) [k]nowingly cause transmission of a program, information, code, or command, and (2) intentionally cause damage to protected computer without authorization."[135] To implicate sections (a)(5)(B) and (a)(5)(C), one must "[i]ntentionally access a protected computer without authorization" and "recklessly cause damage," or cause damage or loss, respectively.[136] Damage can include physical damage to a computer system or the dismantling of a communication system that prohibits emergency responders from functioning.[137]

Section 1030 (a)(6) outlaws trafficking in passwords for a government computer, or when the trafficking affects interstate or foreign commerce.[138] Section (a)(7) outlaws threatening to damage a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce.[139] Section 1030 (b) makes it a crime to attempt or conspire to commit any of these offenses.[140] Section 1030 (c) catalogs the penalties for committing them that range from imprisonment for not more than a year for simple cyberspace trespassing to a maximum of life imprisonment when death results from intentional computer damage.[141]

Finally, there are the interesting parts of the CFAA that cause a problem for military cyber activities. Section 1030 (d) preserves the

---

[134] *See* 18 U.S.C. § 1030(a)(5); DOYLE, *supra* note 122, at 29-32; JARRETT ET AL., *supra* note 119, at 35-48.
[135] JARRETT ET AL., *supra* note 119, at 35.
[136] *Id.*
[137] *See* DOYLE, *supra* note 122, at 29-32; JARRETT ET AL., *supra* note 119, at 36.
[138] *See* 18 U.S.C. § 1030(a)(6); DOYLE, *supra* note 122, at 68-70; JARRETT ET AL., *supra* note 119, at 49.
[139] *See* 18 U.S.C. § 1030(a)(7); DOYLE, *supra* note 122, at 2; JARRETT ET AL., *supra* note 119, at 52.
[140] *See* 18 U.S.C. § 1030(b); DOYLE, *supra* note 122, at 2; JARRETT ET AL., *supra* note 119, at 55.
[141] *See* 18 U.S.C. § 1030(c); DOYLE, *supra* note 122, at 2.

investigative authority of the Secret Service.[142] Section 1030 (f) disclaims any application to otherwise permissible law enforcement activities or intelligence activities, thus establishing an exemption for law enforcement or intelligence activities that would otherwise violate the CFAA.[143] Section 1030 (g) creates a civil cause of action for victims of these crimes.[144] "[A]ny person who suffers loss or damage by reason of a violation of" the CFAA may use section (g) to bring a civil cause of action against the actor who violated the CFAA, where person is defined as "any individual, firm, corporation, educational institution, governmental entity, or legal or other entity."[145] Additionally, there is a broad definition for the types of losses covered under section (g). And because the CFAA covers all "protected computers," which, as mentioned above, is broadly defined, the jurisdiction for such claims is wide.

III. DO MILITARY ACTIONS IN CYBERSPACE VIOLATE THE CFAA?

A. U.S. Military Cyber Activities

Joint Publication 3-12(R): Cyberspace Operations ("JP 3-12") is the military's doctrine for synchronizing the military's operations in cyberspace. The Joint Staff, J3 Operations division maintains this doctrine and promulgates it throughout the military and all of the services to provide guidance on military cyberspace operations. JP 3-12 states that military "[c]ommanders conduct cyberspace operations ("CO") to retain freedom of maneuver in cyberspace, accomplish the joint force commander's objectives, deny freedom of action to adversaries, and enable other operational activities."[146] JP 3-12 names three categories of cyberspace

[142] *See* 18 U.S.C. § 1030(d)(1); DOYLE, *supra* note 122, at 2.
[143] *See* 18 U.S.C. § 1030(f); DOYLE, *supra* note 122, at 2. *See also* Letter from John O. Brennan, Dir., Cent. Intelligence Agency, to Senator Ron Wyden, Cent. Intelligence Agency (Feb. 3, 2014), http://www.wyden.senate.gov/download/?id= 0a7dcd9a-d768-473c-937c-cb47ec3ac966&download=1 (explaining that 18 U.S.C. § 1030(f) allows the Central Intelligence Agency the ability to conduct any lawful investigation necessary).
[144] *See* 18 U.S.C. § 1030(g); DOYLE, *supra* note 122, at 2.
[145] DOYLE, *supra* note 122, at 24.
[146] JP 3-12, *supra* note 2, at vi.

operations that the military carries out: (1) offensive cyberspace operations ("OCO"), (2) defensive cyberspace operations ("DCO") and DOD information network operations.[147]

OCO are CO intended to project power by the application of force in and through cyberspace. DCO are CO intended to defend DOD or other friendly cyberspace. DODIN operations are actions taken to design, build, configure, secure, operate, maintain, and sustain DOD communications systems and networks in a way that creates and preserves data availability, integrity, confidentiality, as well as user/entity authentication and non-repudiation.[148]

JP 3-12 enumerates several threats that it intends to counter with this combination of CO. First, there is the Nation State threat, where "[o]ther nations may employ cyberspace to either attack or conduct espionage against the U.S."[149] The second threat, the Transnational Actor threat, involves "actors [that] use cyberspace to raise funds, communicate with target audiences and each other, recruit, plan operations, destabilize confidence in governments, and conduct direct terrorist actions within cyberspace."[150] The third threat, Criminal Organization, uses cyberspace to "steal information for their own use or, in turn, to sell to raise capital."[151] Additionally, criminal organizations may also "be used as surrogates by nation states or transnational actors to conduct attacks or espionage through [cyber operations]."[152] The fourth threat, Individual Actors or Small Groups can gain "access into systems to discover vulnerabilities, sometimes sharing the information with the owners; however, they also may have malicious intent."[153] Because Individual Actors and Small Groups are often driven by strong political points of view, cyberspace provides an easy way to spread their message. "These actors can be exploited by others, such as criminal organizations or nation states, in order to execute concealed

[147] *Id*. at vii.
[148] *Id*.
[149] *Id*. at I-6.
[150] *Id*. at I-7.
[151] *Id*.
[152] JP 3-12, *supra* note 2, at I-7.
[153] *Id*.

operations against targets in order to preserve their identity or create plausible deniability."[154]

JP 3-12(R) does not reveal much about the OCO used by the military to engage these threats; however, it does mention, "OCO are CO intended to project power by the application of force in and through cyberspace."[155] Additionally, OCO require authorization "like [traditional military] offensive operations in the physical domains, via an execute order" and must be conducted in accordance with current policies.[156] "DCO are CO intended to defend DOD or other friendly cyberspace."[157] DCO are both passive and active CO designed to "preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems."[158] DCO Response Actions "must be authorized in accordance with the standing rules of engagement and any applicable supplemental rules of engagement and may rise to the level of use of force."[159] JP 3-12(R) encourages cyber activities to "be in compliance with U.S. domestic law, international law, and applicable rules of engagement."[160]

JP 3-12(R) also explains the type of capabilities that the military might exploit in cyberspace. Cyberspace defense is one such capability, which includes activities such as "protect[ing], detect[ing], characterize[ing], counter[ing], and mitigat[ing]" actions taking place in cyberspace.[161] Cyberspace intelligence, surveillance, and reconnaissance ("ISR") is an action "conducted to gather intelligence that may be required to support future operations, including OCO or DCO."[162]

---

[154] *Id.*
[155] *Id.* at II-2.
[156] *Id.*
[157] *Id.*
[158] JP 3-12, *supra* note 2, at II-2.
[159] *Id.* at II-3.
[160] *Id.*
[161] *Id.* at II-4.
[162] *Id.* at II-5.

Cyberspace attacks are "actions that create various direct denial effects in cyberspace (i.e., degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains."[163] Cyberspace attacks that fall under the category of "denial" are designed to "degrade, disrupt, or destroy access to, operation of, or availability of a target by a specified level for a specified time."[164] Within such attacks, to "degrade" access means to "deny access to, or operation of, a target to a level represented as a percentage of capacity."[165] To "disrupt" means to "completely but temporarily deny access to, or operation of, a target for a period of time."[166] And to "destroy" means to "permanently, completely, and irreparably deny access to, or operation of, a target."[167] Manipulation attacks aim to "control or change the adversary's information, information systems, and/or networks in a manner that supports the [military's] objectives."[168]

Based on DOD's policy regarding cyber operations and CYBERCOM's mission, DOD's current CO may conflict with its need for DOD actions to comply with domestic and international legal frameworks governing cyberspace. While DOD may be justified in responding to a cyber attack against the United States., some of the DOD operations described likely violate the CFAA. Thus, if the CFAA applies to DOD and members of the armed forces, U.S. military personnel may find themselves personally liable for the cyber activities they conduct, despite carrying out those activities in accordance with their orders.

B. Interpreting the CFAA: Is the Military Acting in Violation of the Law?

When examining the CFAA, one thing is evident: 18 U.S.C. § 1030 (f) creates an exception that states "[t]his section does not prohibit any lawfully authorized investigative, protective, or

[163] *Id.*
[164] JP 3-12, *supra* note 2, at II-5.
[165] *Id.*
[166] *Id.*
[167] *Id.*
[168] *Id.*

intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States."[169] As the military increases its role in cyberspace and potentially takes actions that may violate the CFAA, determining whether this exception applies to DOD is critical. After all, the United States does not hold members of the armed forces personally liable for violating other laws, such as when members of the armed forces are handed weapons and told to kill enemy combatants.[170] Thus, CYBERCOM's success in meeting its objectives may turn on whether members of the armed services are violating the CFAA and whether members of the armed services may be held civilly liable for the actions undertaken by the DOD.[171]

This analysis will begin by examining judicial precedent on the applicability of federal laws to government agents and whether members of the military may be held personally liable for acting in accordance with their orders. The analysis will continue by applying canons of statutory interpretation to the text of the CFAA. The analysis will then use various methods of statutory interpretation, to include plain meaning and new textualism, pragmatism, and legislative intent, in determining whether the Supreme Court would find that the military's cyber activities violate the CFAA. The analysis ultimately concludes that the military is likely violating the CFAA and suggests a way forward to resolve this potential problem and avoid holding soldiers, sailors, airmen, and marines personally liable for merely following orders.

Nardone v. United States is an excellent place to begin the analysis assessing the applicability of the CFAA to DOD cyber

[169] Computer Fraud and Abuse Act, 18 U.S.C. § 1030(f) (2008).
[170] DYCUS ET AL., *supra* note 4, at 404.
[171] Where military personnel are operating under the authority of intelligence agencies, they are covered by the exception. *See* 18 U.S.C. § 1030(f). This occurs when military personnel are stationed—or their permanent duty station is— at one of the intelligence agencies. However, as CYBERCOM has its own mission and authorities, whether DOD's actions violate the CFAA is a key concern. CYBERCOM must also act in accordance with domestic law and international law governing conduct at war. *See* Exec. Order No. 12,333, 46 F.R. 59941 (1981).

activities.[172] *Nardone* explains that when the legislature fails to create an exception for the activities of the government or government agents, activities undertaken by such agents that violate the statute are impermissible.[173] In *Nardone*, the Supreme Court was analyzing the Federal Communications Act of 1934.[174] The statute provides that

> no person who, as an employee, has to do with the sending or receiving of any interstate communication by wire shall divulge or publish it or its substance to anyone other than the addressee or his authorized representative or to authorized fellow employees, save in response to a subpoena issued by a court of competent jurisdiction or on demand of other lawful authority; and "no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person."[175]

The Court found that because the statute read "no person" and did not create any exceptions for agents of or for the federal government, the statute prohibited wiretapping by all persons, including federal agents of the government, even when doing so for investigative purposes.[176] The evidence federal agents obtained to prosecute Nardone and his conspirators for alcohol smuggling during Prohibition was inadmissible because the agents had knowingly violated the Federal Communications Act of 1934 to obtain it.[177] Two years later, the Court further held that a summary of the general content, not only the exact wording of the messages, was also inadmissible as it was also illegally obtained.[178] The content was the "fruit of the poisonous tree;" thus, what the government had

[172] Nardone v. United States, 302 U.S. 379, 379 (1937).
[173] *Id*. at 383.
[174] *Id*. at 380-81.
[175] *Id.*
[176] *Id*. at 384-85.
[177] *Id*. at 389.
[178] Nardone v. United States, 308 U.S. 338, 340-41 (1939).

wrongfully obtained was inadmissible regardless of whether it was the exact words or a summary of the content.[179]

The Court, in the first *Nardone* case, held that if Congress desired to permit the government or government agents to act contrary to the statute, Congress was more than capable of writing such an exception into the act.[180] However, the Court found that "Congress may have thought it less important that some offenders should go unwhipped of justice than that officers should resort to methods deemed inconsistent with ethical standards and destructive of personal liberty." Thus, the Court relied on the plain words of the statute and Congress's intent to protect personal liberty.[181] The Court found that where Congress had created no exception, the government could not act contrary to the statute.[182]

The *Nardone* cases set a strong precedent for general applicability statutes: where Congress creates no exception for the government or government agents, activities conducted by the government or its agents that violate the statute are impermissible. Thus, the words of the statute bind the conduct of the federal government, or the agents thereof, the same way they bind any other person.

Moreover, in *Little v. Barreme*, a Supreme Court case from 1804, the Court found that members of the military may be held personally liable for damages caused to any person injured by their actions, even if the actions were in accordance with their orders.[183] In *Little*, a ship captain was found liable for civil damages when he seized a ship coming from a French port on direct orders from the President, the Commander in Chief, because such actions exceeded the statutory authority granted for seizing ships.[184] The statutory authority permitted the seizing of ships going to a French port; when the orders were given, however, the executive expanded them to

[179] *Id.*
[180] Nardone v. United States, 302 U.S. 379, 381-83 (1937).
[181] *Id.* at 384-85.
[182] *Id.*
[183] Little v. Barreme, 6 U.S. 170, 179 (1804).
[184] *Id.* at 177-78.

include ships going to and coming from a French port.[185] Chief Justice Marshall explained that it seemed logical to hold the issuing authority responsible for the liabilities arising from the actions of military officers following their instructions, as it is the duty of military personnel to obey orders.[186] However, the Chief Justice further explained that the fact that a military member was merely following orders did not change the nature of the actions or legalize an act that exceeded the statutory authority granted by the legislature.[187] Thus, the Court found the captain to be personally liable for the damages.[188]

Little stands for the proposition that military personnel may be held liable for damages caused by their actions when such actions violate statutory law, even if the actions are taken in accordance with military orders. Although *Nardone* is from the 1930's and *Little* from the 1800's, both still stand as applicable law. Taken together, there is a strong precedent for holding members of the armed forces personally liable for their actions, even when acting in accordance with orders, when those actions violate valid statutory law.

In *Legislation and Statutory Interpretation*, authors William N. Eskridge, Philip P. Frickey, and Elizabeth Garret explain that there is a "super strong presumption of correctness" when the Court interprets statutes and creates precedent for interpreting statutes.[189] "Once the Supreme Court has authoritatively construed a federal statute, that precedent is not only entitled to the usual presumption of correctness suggested by the common law doctrine of *stare decisis*, but it is supposed to be given an even stronger *stare decisis* effect."[190] Furthermore, the Court believes that when its interpretation is

[185] *Id.*
[186] *Id.* at 179.
[187] *Id.*
[188] *Id.*
[189] WILLIAM N. ESKRIDGE ET AL., LEGISLATION AND STATUTORY INTERPRETATION 284 (2nd ed. 2006).
[190] *Id.* at 286.

wrong, Congress, rather than the Court, is responsible for fixing the meaning of the statute.[191]

Given precedent, and the Court's deference in accordance with the principle of *stare decisis*, it is likely that the Court would hold members of the armed services who conduct cyber activities that violate the CFAA personally liable for those activities. It is possible to argue that because the CFAA creates an exception for some government activity (the section 1030 (f) exception for law enforcement and intelligence activities), the *Nardone* general applicability rule does not apply to the CFAA. This, however, fails to incorporate the notion of *expressio unius est exclusio alterius ("expressio unius")*. This canon of statutory interpretation translates to and means, "the expression of one thing suggests exclusion of all others."[192] The Court relies on canons of interpretation to help create consistency in interpretation of statutes.[193]

Thus, in following the Court's logic in *Nardone* and employing the *expressio unius* canon, Congress's failure to create an exception for the military while creating an exception for law enforcement and intelligence activities implies that the military cannot make use of the exception. After all, had Congress wanted to include the military in the exception, it easily could have done so when it created an exception for two other forms of government—law enforcement and intelligence activities. The fact that Congress created an exception for certain aspects of the federal government does not imply that all government agencies, departments, or agents may make use of the exception. In fact, it would seem to be the opposite. If Congress legislates certain, limited exceptions rather than generally excusing government activities, it conveys the intent to limit the exceptions only to what Congress expressly grants.

Furthermore, when examining the text of the CFAA under a new textualist approach, the plain meaning is that Congress did not grant the military an exception for cyber activities that ostensibly

[191] *Id*.
[192] *Id*. at 263.
[193] *Id*. at 260.

violate the CFAA. New textualists believe that the meaning of statutory text should be derived from "the meaning an ordinary speaker of the English language would draw from the statutory text."[194] According to new textualists, "the only thing that actually becomes law is the statutory text, [and] any unwritten intentions of one House of one committee or of one member are not law."[195] Under this theory, "when the text is relatively clear, interpreters should not even consider other evidence of specific legislative intent or general purpose."[196] The plain meaning of the CFAA, from a new textualist perspective, indicates that Congress wanted to create a limited exception for certain government activities. From this perspective, the CFAA makes clear that some elements of the government are exempt from complying with the statute. The military however, is not included in 18 U.S.C. § 1030 (f).

It is possible to argue pragmatically, using a dynamic theory, to find an exception for the military implied in section 1030 (f).[197] After all, the statutory text does not exist in isolation and given the likely good intentions of military cyber activities, it might make sense to imply an exception for military activities when one already exists for similar government actions. However, given the strong precedent and plain meaning of the text, these arguments would likely fail. Because the "rule of law requires a law of rules that are predictable applied to everyone," deciding based on arguments that do not comport to the plain meaning of the text would essentially be deciding against what has become law.[198] The Constitution set up a rigid process for creating law—the process of Bicameralism and Presentment—that was designed to create well-reasoned laws.[199] Through this process, Congress created a limited exception without extending 18 U.S.C. § 1030 (f) to the military. Thus, finding an exception where none exists would go against judicial precedent, plain meaning, and the text of the statute that became law.

---

[194] *Id*. at 235-36.
[195] ESKRIDGE ET AL., *supra* note 189, at 235-36.
[196] *Id*.
[197] *Id*. at 245-50.
[198] *Id*. at 237.
[199] *Id*.

While the original intent of the CFAA may have been narrowly tailored for the protection of government computers and prohibiting access to sensitive government information, its continuous evolution through numerous amendments has drastically changed its reach and intent.[200] As previously mentioned, the CFAA reaches almost every computer and every computer user because of the ever-growing cyber security threat.[201] Thus, while law enforcement and intelligence activities have remained in the 18 U.S.C. § 1030 (f) exception, the legislature has failed to extend that exception to the military. As the DOD's role in cyber security continues to grow and expand, a problem arises because of the CFAA's liabilities and the statute's likely applicability to U.S. military personnel. While the United States does not hold members of the military liable for other offenses committed in violation of domestic or international law when acting in accordance with their orders, military personnel may find themselves liable under the CFAA.

IV. THE SOLUTION

A. A Quick Fix

The obvious quick fix is to add the military to the Section 1030 exception or amend the statute adding a new exception for the military. This conclusion seems logical, given the wording of 18 U.S.C. § 1030 (f), which permits lawful investigative, protective, and intelligence cyber activities of law enforcement and intelligence agencies. Thus, lawfully authorized, investigative, protective, and intelligence activities, or those similar in nature, carried out by the armed forces to protect and defend the United States seem to qualify for the same exception. This solution, however, is dependent on Congress's determination that the military should be exempted from CFAA liability.

---

[200] *See, e.g.*, Major Christopher M. Kessinger, *Hitting the Cyber Marque: Issuing a Cyber Letter of Marque to Combat Digital Threats*, 2013 ARMY LAW. 4, 15 (2013) (explaining that the CFAA now includes civil liability for anyone who "intentionally access[es] a protected computer without authorization or exceed[s] authorized access") (quoting the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(4) (2008)).

[201] *See* JARRETT ET AL., *supra* note 119, at 4; DYCUS ET AL., *supra* note 4, at 267-375.

Congress could also choose to define an exception for the military by granting the military a specific exception for certain DOD activities under the CFAA. Because the military is already operating in cyberspace in ways that potentially violate the CFAA, this exception is necessary, even if it is only temporary. This will enable the military to continue operating without violating the statute and potentially creating civil liabilities for U.S. servicemen and women.

B. The Computer Fraud and Abuse Act

More importantly, Congress should revise the CFAA to reflect its original intent more closely, which was to protect government computer systems and sensitive government information. Because of the CFAA's evolution over the last thirty years, its coverage has become immensely broad; some would argue that it has become so over encompassing that a court should hold it void for vagueness.[202] Congress originally enacted the CFAA with limited applicability.[203] Revising the CFAA so that it resembles this original intent is necessary. Such a modification reflects a more reasonable standard without neglecting the problems the CFAA sought to prevent—most notably, possible attacks on USG computer systems and the loss of sensitive government information. Ignoring this step in the solution exposes more than just the members of the armed forces to potential liabilities. Currently, the statute regulates computer activities of which the average computer user is likely unaware.

More drastically, scrapping the CFAA entirely to replace it with a statute reflecting the more limited, original intent would add clarity to the overly broad statute. Congress could also draft a statute that avoids exposing members of the military to civil liabilities.

C. The Military's Role in Cyber Security

The military's role, and the larger DOD role, in cyberspace needs to be more clearly defined. Domestically, there are a number

[202] Kerr, *supra* note 5, at 1562.
[203] *Id.*

of actors involved in the cyber security debate ranging from the President, to Congress, to the DHS and beyond. Additionally, the volume of applicable statutory material makes it difficult to determine what rules apply to cyberspace and what actions DOD can take that do not violate other federal laws (a main problem underlying the CFAA debate). Moreover, although cyberspace is becoming a major concern for the USG and U.S. allies, the international policy on cyberspace is unsettled. Therefore, determining what constitutes a cyber attack, determining an appropriate response to cyber incidents, and determining what actions can be taken offensively and defensively in cyberspace are necessary to create a legal framework for governing this 21st-century battlefield.

Based on the indefiniteness of policy in this area, this is no easy task. However, as the world becomes increasingly reliant on technology and cyberspace, including U.S. adversaries, and incidents involving cyberspace continue to occur with increasing frequency, efforts to establish the DOD's role in cyberspace, as well as clarifying the rules of engagement in cyberspace are critical to U.S. national security. And, as this comment demonstrates, it is essential to protecting servicemen and women from civil liabilities for merely following military orders that may violate the law.

V. CONCLUSION

Cyberspace is one of the newest and most challenging battlefields, and it is accompanied by a lack of clear legal standards governing conduct. Because of the unique challenges presented by cyberspace, traditional international law and U.S. domestic law have left a gap in authority for DOD action. As DOD increases its presence in cyberspace, it faces a unique challenge: potential civil liabilities for members of the armed services when acting in accordance with orders that violate the CFAA. The military merits a speedy exception to this statute similar to that provided for law enforcement and the intelligence community. Furthermore, the CFAA needs a revision to embody its original intent to correct its over encompassing expansion after 30 years and many amendments. Finally, defining the military's role in cyberspace and the rules of

engagement for this new battlefield is essential to U.S. national security.