National Security Law Journal

VOLUME 4

ISSUE 2

SPRING/SUMMER 2016

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 2 (SPRING/SUMMER 2016)
ISBN-13: 978-1530877690
ISBN-10: 1530877695

National Security Law Journal

ARTICLES

SYMPOSIUM PANEL

COMMENTS

VOLUME 4 SPRING/SUMMER 2016 ISSUE 2

NATIONAL SECURITY
LAW JOURNAL

PUBLISHED BY GEORGE MASON UNIVERSITY SCHOOL OF LAW

Cite as 4 NAT'L SEC. L.J. ___ (2016).

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 | SPRING/SUMMER 2016 | ISSUE 2

2015-2016 EDITORIAL BOARD

NATIONAL SECURITY
LAW JOURNAL

PUBLISHED BY GEORGE MASON UNIVERSITY SCHOOL OF LAW

FOREWORD

In this issue, Colonel Dawn Zoldi, Captain Joseph Groff, and Captain Gregory Speirs, analyze national security effects of federal preemption and drone laws; and John Bickers, Associate Professor of Law at Northern Kentucky University, examines military commission reversals in terrorism trials and suggests that these reversals occurred because of the inappropriate amalgamation of grave breaches and belligerency offenses. Next, this issue includes a transcript of our Fall 2015 Symposium in which a panel of experts discusses the Department of Defense's Law of War Manual released in the summer of 2015. This issue also contains two Comments by Mason students: Jameson Goodell advocates for the use of the Treason Clause of the Constitution for American recruits supporting terrorist operations on the homeland and abroad, and Chelsea Smith proposes legislation reform to address deficiencies in order to safeguard federal information systems.

I want to thank our Editorial Board for the tremendous effort this year in publishing both of our issues. I also have the utmost confidence in our incoming Editorial Board, and I know you will continue to grow the *National Security Law Journal*, both in membership and reach.

Please connect with us on social media via Facebook (facebook.com/NatlSecLJ), Twitter (@NatlSecLJ), and subscribe to our YouTube channel (youtube.com/NatlSecLJ).

Rick Myers
Editor-in-Chief

NATIONAL SECURITY
LAW JOURNAL

VOLUME 4 | SPRING/SUMMER 2016 | ISSUE 2

CONTENTS

ARTICLES

SYMPOSIUM PANEL

COMMENTS

STATES RIGHTS . . . OR JUST WRONG?

A DISCUSSION OF DRONE LAWS AND NATIONAL SECURITY THROUGH THE LENS OF FEDERAL PRE-EMPTION

Colonel Dawn M.K. Zoldi, Captain Joseph M. Groff and Captain Gregory R. Speirs
United States Air Force*

That drones present a genuine national security threat is no secret. Missing from most analysts' radar, however, is how the lack of a federal regulatory scheme assimilating drones into the national airspace is, in and of itself, a threat to our security. The current patchwork of state and local legislation creates conflicts and leaves gaps in regulation to the detriment of the safe inclusion of drones into the national airspace. These legal and policy conflicts and gaps also exist between the states and our Federal government creating ambiguity and a lack of cohesiveness. Until the FAA releases a comprehensive regulatory framework, integrating appropriate roles for state and local government agencies, the country is ill prepared to respond to emergencies involving drones and risks compounding potential disasters. This article reviews the current statutory collage through the lens of the federal preemption doctrine to discern the

* *The views expressed herein are those of the authors and do not represent those of the U.S. Air Force or the Department of Defense.* Colonel Dawn M.K. Zoldi, USAF (B.A. History and Philosophy, University of Scranton (1989); M.A. History University of Scranton (1989); J.D. Villanova University School of Law (1992); M.S. Military Strategic Studies, Air War College, Air University with Distinction (2010)) is currently the Staff Judge Advocate, United States Air Force Academy (USAFA). Captain Joseph M. Groff, USAF (B.A. History, University of California at Los Angeles; M.P.P. Pepperdine School of Public Policy (2009); J.D. Pepperdine School of Law (2009)) is currently an Assistant Staff Judge Advocate assigned to the United States Air Force Academy. Captain Gregory Speirs, USAF (B.A. International Relations with a concentration in National Security, Pennsylvania State University (2009); J.D. North Carolina Central University School of Law (2014)) is currently an Assistant Staff Judge Advocate stationed at Lackland AFB, TX.

state of the law on drones and its potential impacts on national security.

INTRODUCTION

The skies are filled with drones. Drones have interfered with firefighting efforts in California, crashed-landed at prominent

sporting venues, and been routinely spotted in the same airspace by manned-aircraft.[1] A drone even landed on the White House lawn.[2]

And more drones are on the way. In 2013, the leading drone manufacturing company acquired $131 million in sales revenues.[3] They earned an estimated $500 million the next year. The annual global drone revenue for 2016 estimates to reach one billion dollars.[4] Drones are projected to become a multi-billion-dollar industry.[5]

As drones proliferate across the country, powers once reserved for the nation's air forces, such as mobility, speed, range and altitude, are within the purview of radio-controlled aircraft hobbyists.[6] Yet the regulatory landscape has failed to keep pace with technological development. Federal Aviation Administration ("FAA") rulemaking to assimilate drones into the national airspace ("NAS") has lagged. In response, the states have attempted to fill the void. The result is a patchwork of conflicting guidance, coupled with gaping legal holes.

The purpose of this article is not to review the potential threat to national security posed by drones, but rather to posit that in the wake of the democratization of airpower to individual users, the lack of clear regulation is, in and of itself, a threat to national

---

[1] 80 F.R § 78594 (2015).
[2] Interview by Fareed Zakaria with Barack Obama, President, United States (Jan. 27, 2015), http://cnnpressroom.blogs.cnn.com/2015/01/27/presidentobamainterviewedbycnnsfareedzakariainindiaforcnnsnewday/.
[3] Alan Levin, *Santa Delivering Drones for Christmas Amid Rising Safety Concern*, BLOOMBERG BUS. (Dec. 17 2014), http://www.bloomberg.com/news/articles/2014-12-17/santa-delivering-drones-for-christmas-amid-rising-safety-concern.
[4] Gail Whitney, *3 Drone Stocks to Watch in 2016*, UAV EXPERT NEWS (Dec. 22, 2015), http://www.uavexpertnews. com/3-drone-stocks-to-watch-in-2016/.
[5] Clay Dillow, *What Is The Drone Industry Really Worth?*, FORTUNE (Mar. 12, 2013), http://fortune.com/2013/03/ 12/what-is-the-drone-industry-really-worth/.
[6] *Unmanned Aerial System Threats: Exploring Security Implications and Migration Technologies: Hearing before the Subcomm. on Oversight and Mgmt. Efficiency of the Comm. on Homeland Security*, 114th Cong. 15-16 (2015) (testimony of Maj Gen. Fred Roggero, USAF Ret.).

security. As will be discussed, the current patchwork of state legislation creates conflicts and leaves gaps in regulation to the detriment of the safe inclusion of drones into the NAS. These legal and policy conflicts and gaps exist, not just between the states, but also between the states and our Federal government creating ambiguity and a lack of cohesiveness, including in response to emergencies such as terrorist attacks. Thus, this article reviews federal drone regulations and state statutes through a pre-emption lens, to discern the current state of the law and its potential impacts on national security.

Part I begins this analysis with a brief overview of federal pre-emption law. Part II continues on to review current federal aviation laws and proposed FAA regulations relevant to drone use in the NAS. Part III addresses state laws relating to drone use, highlighting topics rightly regulated by the states and those normally reserved for federal action under pre-emption doctrine. Part IV, navigates the legal seams, conflicts, and gaps to illustrate how the ensuing legal ambiguity creates a veritable safe-haven for bad actors. Finally, Part V concludes by summarizing the problem and suggesting that a comprehensive federal approach to drone regulation is the best approach to protect our nation's security.

I. FEDERAL PRE-EMPTION LAW

A. Pre-emption Doctrine

In *McCulloch v. Maryland*, the Supreme Court determined that Article VI, clause 2, of the United States Constitution, commonly referred to as the "Supremacy Clause," enshrined the idea that all valid laws enacted by Congress cannot be impeded, burdened or contradicted by state law.[7] Pre-emption is the concept that inconsistent state laws will fall, null and void, in light of existing federal law on the same issue. Federal regulations are considered to be an extension of Congressional legislative intent and have the same

[7] McCulloch v. Maryland, 17 U.S. 316, 405-06 (1819).

pre-emptive effect as enacted statutes.[8] However, any pre-emption analysis begins with the "assumption that the historic police powers of the States [are] not to be superseded by . . . Federal Act unless that [is] the clear and manifest purpose of Congress."[9]

The intention of Congress to pre-empt exists in a number of ways. The courts have identified three different ways federal pre-emption occurs: express, conflict, and field pre-emption. Express pre-emption occurs when Congressional intent to pre-empt is "explicitly stated in the statute's language."[10] This puts the states on clear notice of federal intent to occupy an area of law and to prevent the enforcement of any state or local laws to the contrary. Conflict pre-emption exists when a state law impedes, burdens, or controverts the intent of the federal law, or when compliance with both federal and state law becomes impossible.[11] In such a case, any state law that conflicts with a valid federal law is void. When neither express nor conflict pre-emption are present, state law is still pre-empted when a federal regulatory scheme is "so pervasive as to make reasonable the inference that Congress left no room for the states to supplement it," or when "the Act of Congress may touch a field in which the federal interest is so dominant that the federal system will be assumed to preclude enforcement of state laws on the same subject."[12] In these instances, courts conclude that field pre-emption applies. Likewise, any state law existing in the field addressed by the federal scheme is void.

B. As Applied to Aviation

With passage of the Federal Aviation Act of 1958 ("Aviation Act"), the United States declared exclusive sovereignty over its NAS

---

[8] *See* Nat'l Meat Ass'n v. Harris, 132 S. Ct. 965, 970-71 (2012); Fid. Fed. Sav. & Loan Ass'n v. de la Cuesta, 458 U.S. 141, 153 (1982); United States v. Shimer, 367 U.S. 374, 381-82 (1961).

[9] Rice v. Santa Fe Elevator Corp., 331 U.S. 218, 230 (1947).

[10] Cipollone v. Liggett Group, 505 U.S. 504, 516 (1992) (quoting Jones v. Rath Packing Co., 430 U.S. 519, 525 (1977)).

[11] *See Fid. Fed. Sav. & Loan Ass'n*, 458 U.S. at 153.

[12] *See Rice*, 331 U.S. at 230.

and set the course for field pre-emption of its safe and efficient use.[13] The Aviation Act established the FAA as the centralized authority with the power to frame the rules for operating in the NAS.[14] Even so, the courts have not held that the FAA has acted so comprehensively that the entire field of aviation is pre-empted, as the mere volume and complexity of the FAA's regulatory scheme is not alone determinative.[15]

The Supreme Court, in cases that have implicated the Aviation Act, has looked first to the FAA's overarching mandate to regulate the use of the navigable airspace, then specifically as to whether or not the FAA's regulations in each particular aspect of aviation demonstrate an intent to occupy that particular field.[16] For example, in *Burbank v. Lockheed Air Terminal, Inc.*, the Court interpreted the Aviation Act, as amended by the Noise Control Act of 1972 and its implementing regulations, to find that the City of Burbank, California was pre-empted from imposing a curfew on jets between the hours of 11:00 p.m. and 7:00 a.m.[17] The Court's multi-faceted examination of pre-emption led it to conclude that the local curfew was pre-empted, not only because the federal scheme for regulating aircraft noise was pervasive, but also because the collateral impacts of the regulations resulted in cluttering the NAS with flights during the final hours prior to the curfew which negatively impacted the FAA's core responsibility for operational safety.[18]

While the Aviation Act predominantly pre-empts the field of airspace navigation, operations, and safety, the Airline Deregulation Act of 1978 ("ADA") added an express pre-emption clause, prohibiting the states from enforcing any law "relating to rates,

---

[13] *See* Federal Aviation Act of 1958, Pub L. No. 85-726, 72 Stat. 731 (1958); 49 U.S.C.S. § 40103(a)(1) (2016).
[14] United States v. Christensen, 419 F.2d 1401, 1404 (9th Cir. 1969); Air Line Pilots Ass'n v. Quesada, 276 F.2d 892, 894 (2d Cir. 1960).
[15] Skysign Int'l v. Honolulu, 276 F.3d 1109, 1116-17 (9th Cir. 2002) (citing Hillsborough Cty. v. Automated Med. Labs., 471 U.S. 707, 718 (1985)); Morris v. Cessna Aircraft Co., 833 F. Supp. 2d 622, 630 (N.D. Tex. 2011).
[16] *See generally* Burbank v. Lockheed Air Terminal, Inc., 411 U.S. 624, 625-26, 631-34 (1973).
[17] *Id.* at 626.
[18] *Id.* at 627, 633.

routes, or services" of any air carrier.[19] In 1988, the National Association of Attorneys General ("NAAG") adopted Air Travel Industry Enforcement Guidelines that purported to "explain in detail how existing state laws apply to air fare advertising and frequent flyer programs."[20] These enforcement guidelines were the subject of *Morales v. TWA*, in which the NAAG argued that the express pre-emption clause in the ADA only precluded the states from prescribing actual rates, routes, or services, not the NAAG state-level advertising enforcement scheme. The Supreme Court disagreed and ruled the ADA language expressly pre-empted the guidelines because they "related to" rates, routes, or services. Justice Scalia, writing for the Court, referred to the ADA clause as "broadly worded," "deliberately expansive," and "conspicuous for its breadth," consistent with other similar pre-emption cases, and that such an interpretation by the NAAG would read the words "relating to" right out of the statute.[21]

Thus, with respect to aircraft in the NAS, precedent is clear that the FAA has broad authority to regulate matters affecting operational safety, including noise, as well as air carriers' rates, routes, and services. The FAA Modernization and Reform Act of 2012 ("FMRA") affirmed Congress' intent to apply this aircraft-centric precedent to drones. It also specifically codified the FAA's authority to incorporate drones into the NAS safely.[22] Prior to the FMRA, the FAA treated drones as falling under the umbrella classification of "aircraft," defined as "any contrivance invented, used, or designed to navigate, or fly in, the air."[23] In the FMRA, Congress reaffirmed that a drone is, in fact, an aircraft by defining an unmanned aircraft as "*an aircraft* that is operated without the

[19] Morales v. Trans World Airlines, Inc., 504 U.S. 374, 378-79 (1992) (quoting Airline Deregulation Act of 1978, 49 U.S.C. §1305(a)(1) (1978)).
[20] *Id.* at 379.
[21] *Id.* at 384-85 (quoting a series of ERISA cases: Metro. Life Ins. Co. v. Massachusetts, 471 U.S. 724, 739 (1985); Pilot Life Ins. Co. v. Dedeaux, 481 U.S. 41, 47 (1987); Ingersoll-Rand Co. v. McClendon, 498 U.S. 133, 138 (1990); FMC Corp. v. Holliday, 498 U.S. 52, 58 (1990)).
[22] FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, 126 Stat. 72 (2012).
[23] Definitions, 49 U.S.C. § 40102(a)(6) (2012).

possibility of direct human intervention from within or on the aircraft."[24]

C. As Applied to Drones

The FMRA required the FAA to integrate commercial drones into the NAS by the end of 2015. However, between 2012 and 2015, the rules for drone use remained unclear. By the end of 2015, the FAA had still not finalized its drone regulations. For this reason, and as will be discussed below, the overwhelming majority of states launched their own regulations to address the explosion of public and private drone use, addressing issues ranging from law enforcement use of drones for criminal investigations to licensure and registration requirements. In response, the FAA Office of the Chief Counsel ("OCC") issued a statement addressing federal pre-emption as applicable to state drone laws.[25] Noting the established parameters of the federal regulatory framework charged to and established by the FAA for the safe and efficient use of the NAS, and highlighting the aircraft-centric cases discussed above, the FAA OCC provided examples of the types of state and local laws that they opined were consistent with a state's police powers. These examples included: requiring police to obtain warrants before using drones for surveillance; privacy issues, such as banning drone use for voyeurism; prohibitions for drone use in hunting; or similarly, any type of arming of drones. The OCC requested that state and local authorities consult with the FAA before legislating in the areas of operational drone restrictions on flight altitude, flight paths, or use of navigable airspace, as well as on any mandates on equipment and training related to drone aviation safety. While not a regulation in and of itself, the FAA OCC statement provides useful insight into areas the FAA believes are exclusively within their federal purview. We next turn to a discussion of the current state of the federal FAA rules and regulations applicable to drones in the NAS.

---

[24] Sec. 331(8), 49 U.S.C. § 40101 (2000) (emphasis added).

[25] *See* Fact Sheet, FAA OCC State and Local Regulation of Unmanned Aircraft Systems (UAS) 2 (Dec. 17, 2015) [hereinafter FAA Fact Sheet] http://www.faa.gov/uas/regulations_policies/media/UAS_Fact_Sheet_Final.pdf.

II. FEDERAL AVIATION LAWS AND REGULATIONS APPLICABLE TO DRONES

A. General Aviation Law

As discussed above, the FAA considers drones to be aircraft. Under current federal law, any aircraft operation in the NAS requires a certificated and registered aircraft, a licensed pilot, and operational approval.[26] Unfortunately, the realities of drone operations do not comport with these requirements in many respects largely because the drafters of the Aviation Act and subsequent implementing regulations did not contemplate the use of aircraft that lack an onboard pilot such as drones.

For example, the FAA's current processes for issuing airworthiness and airman certificates, which take between three and five years to complete, were designed to be used for manned aircraft and do not take into account the rate of technological change associated with drones.[27] Likewise, both private, and to a greater extent, commercial pilot certificates require extensive training in aeronautical and operational knowledge from an authorized instructor; specified hours of flight experience (40 for private; 250 for

[26] *See* Operation of Aircraft 49 U.S.C. § 44101 (2015) (civil aircraft registration); Prohibitions and Exemptions, 49 U.S.C. § 44711(a)(1) (2012) (civil airworthiness certificate); 49 U.S.C. § 44711(a)(2)(A) (airman certificate for airman on a civil aircraft being operated in air commerce). These requirements derive from the FAA's definition of "air commerce" and broad administrative and court interpretations of that term that extend coverage to a civil and commercial drone operations. 49 U.S.C. § 40102(a)(3); Administrator v. Barrows, 7 N.T.S.B. 5, 8-9 (1990); United States v. Healy, 376 U.S. 75, 84-85 (1964) (holding that "air commerce" is not limited to commercial airplanes); Hill v. NTSB, 886 F.2d 1275, 1280 (10th Cir. 1989) ("The statutory definition of 'air commerce' is therefore clearly not restricted to interstate flights occurring in controlled or navigable airspace."); United States v. Drumm, 55 F. Supp. 151, 155 (D. Nev. 1944) ("[A]ny operation of any aircraft in the air space either directly affects or may endanger safety in, interstate, overseas, or foreign air commerce.").

[27] FAA, FAA-2015-0150; Notice No. 15-01, Operation and Certification of Small Unmanned Aircraft Systems, DEP'T OF TRANSP. 24-28 (Feb. 15, 2015), https://www.faa.gov/regulations_policies/rulemaking/recently_published/media/2120-AJ60_NPRM_2-15-2015_joint_signature.pdf (notice of proposed rulemaking).

commercial); and a medical certificate, all of which seem unduly burdensome and unworkable for drone operations.[28] Most importantly, because drones do not have an onboard pilot, they conflict with the critical "see and avoid" requirement applicable to general aircraft.[29] This requires that during flight, *a pilot on board the aircraft* look out of the aircraft, and not be hindered by "cock-pit duties," to observe whether his and other aircraft are on a collision path.[30] It is clear from both the text and the history of the "see and avoid" language that "those provisions did not contemplate the use of technology to substitute for the human vision."[31] These are but a few of the significant mismatches between the needs of drone operators and current FAA regulations written with manned flight in mind. Because the current laws are not a perfect fit for drone operations in the NAS, and in accordance with the FMRA, the FAA is attempting to carve out new regulatory spaces for them.[32]

B. A Specific Regulatory Scheme for Drones

As with manned aircraft, the FAA categorizes drones as public, commercial or civil, or as model aircraft. As will be discussed below, public drone operations are well regulated; regulation of civil and commercial drones has been much more complex and continues to evolve; and a loose set of guidelines govern model aircraft.

---

[28] *See* 14 C.F.R. §§ 61(e)-(f); 14 C.F.R. § 61.23(a)(3)(i); 14 C.F.R. § 61.23(a)(2).

[29] 14 C.F.R. § 91.113(b) requires aircraft operators to maintain vigilance "so as to see and avoid other aircraft" and aircraft collision-awareness problems by requiring that a pilot on board the aircraft look out of the aircraft during flight to observe whether other aircraft are on a collision path with his or her aircraft.

[30] Pilot Vigilance, 33 Fed. Reg. 10505 (proposed July 24, 1968) (to be codified at 14 C.F.R. § 91).

[31] U.S. DEP'T OF TRANSP., FAA Notice of Proposed Rulemaking to 14 C.F.R. §§ 21, 43, 45, 47, 61, 91, 101, 107, and 183, at 22 (Feb. 15, 2015).

[32] *See* FAA Notice of Policy: Unmanned Aircraft Operations in the National Airspace System, 27 Fed. Reg. 6689 (Feb. 13, 2007) (to be codified in 14 C.F.R. § 91) (the FAA acknowledges that regulatory standards need to be developed to enable current technology for unmanned aircraft to comply with Title 14 Code of Federal Regulations).

1. Public Drones

Public aircraft, and thus public drones, are defined as, "an aircraft operated by a governmental entity (including federal, state, or local governments, and the U.S. Department of Defense and its military branches) for certain purposes."[33] Public drones obtain access to operate within the NAS through FAA-approved Certificates of Waiver or Authorization ("COA"), an authorization for a specific activity that the FAA provides after operational and technical review of the drone mission.[34] In addition to a COA, public drones also have certification and registration requirements as well as the requirement that licensed pilots operate them.[35]

2. Civil and Commercial Drones

Civil drone operations include any activity that "does not meet the criteria for public Unmanned Aircraft System ("UAS") operations or model aircraft operations."[36] The FAA currently authorizes civil drone operations through a couple of different mechanisms: a grant of exemption to the airworthiness certificate requirement under Section 333 the FMRA ("Section 333 approval"); through a Special Airworthiness Certificate ("SAC") in the Experimental or Restricted Category; or through a special flight permit.[37] Section 333 allows the FAA to provide a case-by-case

[33] *See* 14 C.F.R. § 1.1 for the complete definition of public aircraft. Permissible public drone use is outlined in 49 U.S.C. §§ 40102(a)(41), 40125.

[34] *See Certificates of Waiver or Authorization (COA)*, FAA, http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/systemops/aaim/organizations/uas/coa/ (last visited Apr. 17, 2016). The FAA has a web-based UAS COA Online System and the turn-time for approvals takes approximately sixty days. *Id.*

[35] 49 U.S.C. § 44101; Prohibitions and Exemption 49 U.S.C. § 44711(a)(1) (2012); 49 U.S.C. § 44711(a)(2)(A).

[36] *See Civil Operations (Non-Governmental)*, FAA, http://www.faa.gov/uas/civil_operations/ (last visited Apr. 17, 2016).

[37] FAA Modernization and Reform Act of 2012**,** Pub. L. No. 112-95, §333(a) (2012), Special Rules for Certain Unmanned Aircraft Systems (directed the Secretary of Transportation to determine whether drone operations posing the least amount of public risk and no threat to national security could safely be operated in the NAS and if so, to establish requirements for the safe operation of these systems in the NAS, prior to completion of the UAS comprehensive plan and rulemakings). *See*

approval of commercial drone operations in low-risk and controlled environments prior to the finalization of FAA's Small UAS Rule. Examples of drone operations granted Section 333 approval include real-estate photography and movie cinematography. A time-limited SAC in the Experimental Category applies to research and development, crew training, and market surveys.[38] In the Restricted Category, there are two SAC options, the first of which is an aircraft accepted by an Armed Force of the United States and later modified for a special purpose. Also in the Restricted Category are aircraft used in special purpose operations, such as: agricultural operations; forest and wildlife conservation; aerial surveying; patrolling pipelines, power lines, and canals; weather control; aerial advertising; and "any other operation specified by the FAA."[39] Special flight permits for drones are limited, but include flight-testing of new production aircraft.[40]

In February 2015, the FAA issued a Notice of Public Rule-Making ("NPRM") or proposed rule for drones, up to fifty-five pounds, which would apply only to small commercial drones.[41] The NPRM addresses operational limitations such as daylight-only operations, use of visual observers, confined areas of operation, and visual-line-of-sight operations. Operators must comply with certification requirements that include registration with the Transportation Security Agency and a review for airman certificate applicants. The NPRM also includes aircraft requirements, specifically aircraft registration and marking "in order to maintain

also 14 C.F.R. §§ 21.25(a), 21.197 (2011); FAA Order 8130, 34C (Aug. 2, 2013). Section 333 of Public Law 112-95 directed the Secretary to determine whether UAS operations posing the least amount of public risk and no threat to national security could safely be operated in the NAS and if so, to establish requirements for the safe operation of these systems in the NAS, prior to completion of the UAS comprehensive plan and rulemakings required by section 332 of Public Law 112-95. *See* Pub. L. No. 112-95, §333(a).

[38] 14 C.F.R. §§ 21.191-21.195.

[39] 14 C.F.R. §§ 21.25(a)(2), 21.25(a)(1).

[40] 14 C.F.R. § 21.197 (2010).

[41] *Small UAS Notice of Proposed Rulemaking (NPRM)*, U.S. DEP'T OF TRANSP. (2015) [hereinafter FAA NPRM] ("[T]his proposed rule would…leave the existing public aircraft operations COA process unchanged."), https://www.faa.gov/ uas/nprm/.

the safety of the NAS and ensure that they do not pose a threat to national security."[42] This Rule is not yet finalized.

3. Model Aircraft

FAA Advisory Circular ("AC") 91-57A governs "model aircraft," defined as drones used for "hobby or recreational purposes."[43] It applies only to non-commercial drones and requires conformity with "community-based" or nationwide safety guidelines. Pursuant to AC 91-57A, drone hobbyists must: not interfere with and must give way to manned aircraft; provide notice to Air Traffic Control if any use will be within five miles of an airport; stay out of restricted airspace areas; obey any FAA Temporary Flight Restrictions, and restrict flights below 400 feet.[44] The FAA, in its discretion, has not brought enforcement actions against model-aircraft operations that comply with AC 91-57A.[45]

Although AC 91-57A does not contain registration or certification requirements, the FAA has utilized the "emergency rule-making" provision of the Administrative Procedures Act[46] to issue an Interim Final Rule for Registration and Marking Requirements for Small Unmanned Aircraft.[47] This Rule puts forth the framework for a national drone registry, of anyone at 13 years of age or older to register online for a unique number for drones weighing less than 55 pounds, regardless of intended use.[48]

---

[42] The *Small UAS Notice of Proposed Rulemaking* contained therein provides an excellent synopsis of the major provisions of the NPRM. *Id.* at 10.
[43] FAA, U.S. DEP'T OF TRANSP., AC 91-57A MODEL AIRCRAFT OPERATING STANDARDS—INCLUDING CHANGE 1 (Jan. 11, 2016), https://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentID/1028086.
[44] *Id.*
[45] FAA NPRM, *supra* note 41, at 29.
[46] Rule Making, 5 U.S.C. § 553(b)(3)(B) (2012) (dispensing of the public notice and comment portions of rule-making).
[47] Registration and Marking Requirements for Small Unmanned Aircraft, 80 Fed. Reg. 78,593 (Dec. 16, 2015) (to be codified at 14 C.F.R. pt. 1, 45, 47, 48, 91, and 375).
[48] Registration and Marking Requirements for Small Unmanned Aircraft, 80 Fed. Reg. at 78,595.

Because AC 91-57A does not apply to non-recreational drone operations, until the NPRM is finalized into a Rule, and unless specialized FAA approval is obtained as described above under Section 333 of the FMRA or otherwise, all other non-recreational civil small drone operations are effectively prohibited at this time. What is also currently lacking in FAA's drone regulations, with limited exception, is any reference to large civil UAS.[49]

Until finalization of the Small UAS Rule and other rules that address drones weighing more than 55 pounds, critical issues directly related to national security remain in limbo, such as security vetting for training and certification of drone-related personnel. If the draft Rule is any indication of the anticipated final product, even when it is published, crucial issues will remain unaddressed including cyber and communications vulnerabilities; air defense and domain awareness issues; counter-drone authorities; and other security concerns. Due to the lack of clarity and finality in federal drone regulation, the states have seized the initiative through extensive drone legislation.

III. STATE DRONE LAWS

A. The Landscape

Whereas federal drone regulation has lagged, state legislation has exploded. Between 2013 and 2015, all but one state has proposed a total of approximately 300 drone bills, with roughly one-fifth becoming law.[50] Specifically, 29 states have passed 1 or more bills, totaling 70 laws.[51]

---

[49] Special flight permits only for production flight-testing can be obtained for drones weighing more than 55 pounds. *See* Special Flight Permits, 14 C.F.R. § 21.197 (2015). These will include operational requirements and limitations. *Id.*

[50] Every state except South Dakota has yet to propose a drone bill. *See* Appendix A.

[51] This figure includes Virginia Governor Terry McAuliffe's Executive Order 43. Va. Exec. Order No. 43 (2015). The State lawmaker bills include: H.B. 471, Reg. Sess. (Ala. 2016); H. Con. Res. 6, 28th Leg., 1st Sess. (Alaska 2013); H. Con. Res. 15, 28th Leg., 2d Sess. (Alaska 2014); H.B. 255, 28th Leg., 2d Sess. (Alaska 2014); H.B. 1770, 90th Gen. Assemb., Reg. Sess. (Ark. 2015); H.B. 1349, 90th Gen. Assemb., Reg. Sess. (Ark. 2015); Sen. Con. Res. 16, 2013-14 Reg. Sess. (Cal. 2013); Assemb. J. Res. 6,

State drone laws have focused, to varying degrees on three types of actors: governmental, in particular law enforcement agencies ("LEA"); private; and industry. Forty-four bills that passed directly address LEA or private actors, while sixteen bills are dedicated to test-site establishment, research, development or industry ("RD&I") purposes.[52] Of the 44 non-RD&I laws, 25 are focused on LEAs' use of drones.[53] The remaining 19 address private actors across a wide

2013-14 Reg. Sess. (Cal. 2013); Assemb. B. 856, 2015-16 Reg. Sess. (Cal. 2015); S.B. 766, 2015 Leg., 24th Sess. (Fla. 2015); H.R. 80, 152nd Assemb., Reg. Sess. (Ga. 2013); H.R. 81, 152nd Gen. Assemb., Reg. Sess. (Ga. 2013); S.R. 172, 152nd Gen. Assemb., Reg. Sess. (Ga. 2013); S.B. 1221, 27th Leg., Reg. Sess. (Haw. 2013); S.B. 661, 28th Leg., Reg. Sess. (Haw. 2015); S.C.R. 103, 62nd Leg., Reg. Sess. (Idaho 2013); S.B. 1134, 62nd Leg., Reg. Sess. (Idaho 2013); S.B. 1587, 98th Gen Assemb. (Ill. 2013); H.B. 1652, 98th Gen. Assemb. (Ill. 2013); S.B. 2937, 98th Gen. Assemb. (Ill. 2013); S.B. 44, 99th Gen. Assemb. (Ill. 2015); H.B. 1009, 118th Gen Assemb., 2nd Reg. Sess. (Ind. 2014); S.R. 27, 118th Gen. Assemb., 1st Reg. Sess. (Ind. 2013); H.F. 2289, 85th Gen. Assemb., Reg. Sess. (Iowa 2014); H.B. 1029, 2014 Reg. Sess. (La. 2014); S.B. 183, 2015 Reg. Sess. (La. 2015); Legis. Doc. 25, 127th Leg., 1st Reg. Sess. (Me. 2015); H.B. 100, 433rd Gen. Assemb., Reg. Sess. (Md. 2013); S.B. 370, 435th Gen. Assemb., Reg. Sess. (Md. 2015); H. Res. 87, 97th Leg. (Mich. 2013); H. Res. 280, 97th Leg. (Mich. 2013); S.B. 54, 98th Leg., Reg. Sess. (Mich. 2015); S.B. 55, 98th Leg., Reg. Sess. (Mich. 2015); S.B. 2022, Reg. Sess. (Miss. 2015); S.B. 196, 63rd Leg., Reg. Sess. (Mont. 2013); S. Con. Res. 7, 77th Leg. (Nev. 2013); Assemb. B. 507, 77th Leg. (Nev. 2013); Assemb. B. 239, 78th Leg. (Nev. 2015); S.B. 222, 160th Leg., Reg. Sess. (N.H. 2015); S.B. 744, 2013 Gen. Assemb., Reg. Sess. (N.C. 2013); S.B. 446, 2015 Gen. Assemb., Reg. Sess. (N.C. 2015); H. Con. Res. 3012, 63rd Leg. Assemb., Reg. Sess. (N.D. 2013); S.B. 2018, 63rd Leg. Assemb., Reg. Sess. (N.D. 2013); H.B. 1328, 64th Leg. Assemb., Reg. Sess. (N.D. 2015); Amend. Substitute H.B. 292, 130th Gen. Assemb., Reg. Sess. (Ohio 2013); H.B. 2710, 77th Leg. Assemb., Reg. Sess. (Ore. 2013); H.B. 2534, 78th Leg. Assemb., Reg. Sess. (Ore. 2015); H.B. 2354, 78th Leg. Assemb., Reg. Sess. (Ore. 2015); S.B. 796, 108th Gen. Assemb., Reg. Sess. (Tenn. 2013); H.B. 591, 108th Gen. Assemb., Reg. Sess. (Tenn. 2013); H.B. 1779, 108th Gen. Assemb., Reg. Sess. (Tenn. 2013); S.B. 1892, 108th Gen. Assemb., Reg. Sess. (Tenn. 2013); H.B. 153, 109th Gen. Assemb., Reg. Sess. (Tenn. 2015); H.B. 912, 83rd Leg., Reg. Sess. (Tex. 2013); H. Comm. Res. 217, 83rd Leg., Reg. Sess. (Tex. 2015); H.B. 3628, 84th Leg., Reg. Sess. (Tex. 2015); H.B. 2167, 84th Leg., Reg. Sess. (Tex. 2015); H.B. 1481, 84th Leg., Reg. Sess. (Tex. 2015); S.B. 167, 2014 Gen. Sess. (Utah 2014); H.B. 296, 2015 Gen. Sess. (Utah 2015); H.B. 2012, 2013 Gen. Assemb. (Va. 2013); S.B. 1331, 2013 Gen. Assemb. (Va. 2013); H.B. 2125, 2015 Gen. Assemb. (Va. 2015); H.B. 1301, 2015 Gen. Assemb (Va. 2015); H. B. 2515, 2015 Leg., Reg. Sess. (W.Va. 2015); S.B. 196, 2013-14 Leg., Reg. Sess. (Wis. 2013); Assemb. B. 203, 2013-14 Leg., Reg. Sess. (Wis. 2013).

[52] *See* Appendix A.

[53] Law Enforcement bills and laws: H.B. 255, 28th Leg., Reg. Sess. (Alaska 2013-2014); S.B. 92, 2012-2013 Leg., Reg. Sess. (Fla. 2013); S.B. 1134, 62nd Leg., 1st Reg. Sess. (Idaho 2013); S.B. 1587, 98th Gen. Assemb., Reg. Sess. (Ill. 2013); S.B. 2937,

range of topics.[54] Only four enacted bills simultaneously regulate both LEAs and private actors.[55]

B. Law Enforcement and Privacy

Portions of signed bills include strict rules for drone use by LEAs. The underlying theme of these laws is a fear of "unwarranted surveillance" that would result in a violation of individual privacy. Generally, these laws seem to take a buffet-style approach to well established Fourth Amendment protections and jurisprudence. For instance, Florida Senate Bill 92 requires a warrant in order for a LEA to use a drone to gather evidence or obtain information, but the LEA may do so without a warrant to counter a terrorist attack, track a fleeing felon, or prevent danger to life.[56] However, this Florida law would effectively prohibit the LEA from conducting a drone search in cases where the individual consents to it.[57]

98th Gen. Assemb., Reg. Sess. (Ill. 2013); H.B. 1009, 118th Gen. Assemb., 2d Reg. Sess. (Ind. 2014); H. File 2289, 85th Gen. Assemb., Reg. Sess. (Iowa 2014); Legis. Doc. 25, 127th Leg., 1st Reg. Sess. (Maine 2015); Mont. S.B. 196, 63rd Leg., Reg. Sess. (Mont. 2013); Assemb. B. 239, 78th Leg., Rreg. Sess. (Nev. 2015); S.B. 744, 2013 Gen. Assemb., Reg. Sess. (N.C. 2013); S.B. 402, 2013 Gen. Assemb., Reg. Sess. (N.C. 2013); H.B. 1328, 64th Legis. Assemb., Reg. Sess. (N.D. 2015); H.B. 2710, 77th Legis. Assemb., Reg. Sess. (Ore. 2013); S.B. 796, 106th Gen. Assemb., Reg. Sess. (Tenn. 2013); TENN. CODE ANN. § 39-13-609 (2015); UTAH CODE ANN. § 63G-18-101 (2014); H.B. 2012, 2013 Leg. Sess. (Va. 2013); S.B. 1331, 2013 Leg. Sess. (Va. 2013); VA. CODE ANN. § 19.2-60.1 (2015); H.B. 2012, 2013 Leg. Sess. (Va. 2013); WIS. STAT. § 175.55 (2013); A.B. 203, 2013-14 Sess., (Wis. 2013).

[54] Private Actor bills and laws include: ARK. CODE ANN. § 5-60-103 (2015); CAL. CIV. CODE § 1708.83 (2015); FLA. STAT. § 934.50 (2015); IDAHO CODE § 21-213 (2013); IND. CODE § 34-30-2-146.4 (2014); LA. STAT. ANN. § 14:336 (2014); LA. STAT. ANN. §§ 3:41-47 (2015); MICH. COMP. LAWS § 324.40112 (2015); MICH. COMP. LAWS ANN. § 324.40111c (West 2015); MISS. CODE ANN. §§ 97-29-61, 63 (2015); N.H. REV. STAT. ANN. § 207:57 (2016); N.C. Gen. Stat. § 15A-300.1; OR. REV. STAT. §§ 837.300-390 (2013); TENN. CODE ANN. § 39-13-903 (2015); TEX. GOVT. CODE ANN. §§ 423.001-008 (West 2013); TEX. GOVT. CODE ANN. §§ 411.062, 065 (West 2015); H.B. 2167, 2007 Leg., Reg. Sess. (Tex. 2007); TEX. FAMILY CODE ANN. § 102.006 (West 2007); W. VA. CODE § 20-2-5 (2015).

[55] *See* IDAHO CODE § 21-213 (2013); IND. CODE § 35-33-5-0.5 (2014); S.B. 744, 2013 Leg., Reg. Sess. (N.C. 2013); TEX. GOVT. CODE ANN. §§ 423.001-008 (West 2013).

[56] FLA. STAT. § 934.50 (2015).

[57] *Id.*

In addition to limited use by LEAs, most state drone laws also contain complicated operational and procedural restrictions ranging from high level of approvals to acquire drones to requirements to maintain records and report drone usage to the public. For example, Illinois Senate Bill 1587 requires their LEAs to:

(1) retain images captured by drones for no longer than 30 days unless an ongoing criminal investigation requires retention;

(2) report on a public website the number of drones on hand, the number of crimes investigated with them and details regarding those drone operations; and

(3) limit drone use pursuant to a warrant to a 45 day period. It also limits drone use to twenty-four hours in the case of an emergency.[58]

Out of 15 states with a LEA-focused law enacted, only 2 have kept it simple. Alaska House Bill 255 and Montana Senate Bill 196 included brief statements that the LEA may use a drone to gather evidence in a criminal investigation under the express terms of a search warrant or "in accordance with a judicially recognized exception to the warrant requirement."[59]

C. Private Actors and Crime

In addition to regulating governmental actors, the states have increasingly focused their attention on private actors' drone use over the last several years. In contrast to only 1 bill passed in 2013 that applied to private actors,[60] in 2015, 10 such bills were enacted.[61] Courts are also beginning to see more cases relating to private drone

[58] ILL. COMP. STAT. § 098-0569 (2014).
[59] ALASKA STAT. § 18.65.902 (2014); MONT. CODE ANN. § 46-5-109 (2015).
[60] IDAHO CODE § 21-213 (2013).
[61] ARK. CODE ANN. § 5-60-103 (2015); CAL. CIV. CODE § 1708.83 (2015); FLA. STAT. § 934.50 (2015); LA. STAT. ANN. §§ 3:41-47 (2015); MICH. COMP. LAWS § 324.40112 (2015); MICH. COMP. LAWS ANN. § 324.40111c (West 2015); MISS. CODE ANN. §§ 97-29-61, 63 (2015); TENN. CODE ANN. § 39-13-903 (2015); TEX. GOVT. CODE ANN. §§ 411.062, 065 (West 2015); W. VA. CODE § 20-2-5 (2015).

users flying over others' private property, including cases of retaliation where individuals have shot down drones.[62] Generally, state legislation focused on private drone users has criminalized private behavior in three main areas: flights near critical state infrastructure; drone voyeurism; and drone use in relation to hunting.

By way of illustration, Texas House Bills 912 and 1481 both list certain structures as "critical infrastructure" near which privately operated drones cannot operate. The Texas law also creates two Class C misdemeanors for illegal use of a drone to capture images and for possessing or distributing the image.[63] Similarly, Arkansas and Mississippi have both passed voyeurism prevention bills, making it a felony for anyone who commits a "Peeping Tom" violation with a drone.[64] On the other hand, some state lawmakers have passed broad criminal legislation for drone use, such as North Carolina Senate Bill 744, which states:

> All crimes committed by use of an unmanned aircraft system, while in flight over this State shall be governed by the laws of the State, and the question of whether the conduct by an unmanned aircraft system while in flight over this State constitutes a crime by the owner of the unmanned aircraft system shall be determined by the laws of this State.[65]

Other criminal provisions for private drone use likely resulted from incidents involving spying on hunters or weaponizing drones to facilitate hunting.[66] Of the 70 bills passed relating to drones in general, 5 bills have addressed hunting game, fishing, and

---

[62] Anthony Bellano, *Cape May County Man Pleads Guilty to Shooting Down Drone*, THE OCEAN CITY PATCH, Feb. 12, 2016, http://patch.com/new-jersey/oceancity/cape-may-county-man-pleads-guilty-shooting-down-drone.

[63] TEX. CODE ANN. § 423.002 (2013); TEX. CODE ANN. § 423.00245 (2013).

[64] H.B. 1349, 90th Gen. Assemb., Reg. Sess. (Ark. 2015);
MISS. CODE ANN. § 97-29-61 (2015). Mississippi Senate Bill 2022 imposes a $5,000 fine for violation of such an act and prison for not more than five years.

[65] N.C. GEN. STAT. § 14-7.45 (2014).

[66] *New Mexico Taking Aim Drones In Hunting Big Game Animals,* ASSOC. PRESS (May 3, 2014), http://www.summitdaily.com/news/11267861-113/drones-hunting-animal-drone.

trapping in some manner.[67] Common language includes prohibitions from "using UAS to interfere with or harass an individual who is hunting."[68]

From a national security standpoint, drone laws that address private users have relatively insignificant ramifications for violating their provisions. Excluding felonious voyeurism, the remaining bills categorize criminal drone use as a misdemeanor. Most are Class C Misdemeanors, which impose no jail time and have maximum fines less than the drone's purchase price.[69]

Drone prosecutions have been few and far between, as a few cases from 2015 illustrate. Most cases involve use of a drone in the commission of an already existing felony or interference with law enforcement or municipal activities. In Maryland, two people were arrested while using a drone in an attempt to smuggle drugs and pornography into a maximum-security prison.[70] In another case, an operator was charged with assault with a deadly weapon after he flew a drone too close to a Los Angeles Police Department chopper.[71] In an upstate New York case, a man was found not guilty of unlawful surveillance in the second degree for allegedly viewing patients in a hospital with his drone.[72]

---

[67] MICH. COMP. LAWS § 324.40112 (2015); MICH. COMP. LAWS § 324.40111c (2015); N.H. REV. STAT. ANN. § 207:57 (2016); OR. REV. STAT. § 498.128 (2015); W.VA. CODE § 20-2-5 (2015).

[68] *See, e.g.*, MICH. COMP. LAWS § 40112.

[69] Misdemeanor penalties: 720 ILL. COMP. STAT. 5/48-3 (2013); IND. CODE § 35-46-8.5(b) (2014) (electronic surveillance as a misdemeanor); N.C. GEN STAT. § 15A-300.1 (2014); TENN. CODE ANN. § 39-13-4 (2013); TEX. GOV'T CODE ANN. § 423 (West 2013).

[70] Kurt Brooks, *2 Arrested in Plot to Fly Contraband Into Prison With Drone,* USA TODAY (Aug. 24, 2015), http:// www.usatoday.com/story/news/nation/2015/08/24/2-arrested-plot-fly-contraband-into-prison-drone/32306943/.

[71] Miriam Hernandez, *Drone Operator Taken Into Custody After Close Call With LAPD Helicopter in Hollywood,* ABC 7 KABC (Aug. 28, 2015), http://www.abc7.com /960511/.

[72] *Man Arrested for Flying Drone Outside Hospital Windows: "I Am Not A Peeping Tom!"*, INSIDE EDITION (Sept. 4, 2015), http://www.insideedition.com/ headlines/11796-man-arrested-for-flying-drone-outside-hospital-windows-i-am-not-a-peeping-tom.

Similarly, the FAA has been slow to take action on regulatory violators, when the local prosecutors fail to act. In one of the rare cases of enforcement, for example, in 2013, the FAA fined a private actor for a drone flight in New York that flew above several buildings and crashed into the sidewalk during rush hour.[73] A businessman standing nearby recovered the drone's chip, which led to the identification of the operator.[74] He handed it to a New York Police officer, who allegedly did not know how to handle the situation.[75] Ultimately, the FAA fined the operator $2,200 because he "endangered the safety of the national airspace system" by flying in a "careless and reckless manner."[76] While New York did not have a statute specifically addressing drones, the police filed the investigation under reckless endangerment before the FAA administered the fine. This is but one of many examples that highlight the lack of an overarching system or process between local governments and the FAA that addresses threats to public safety and security.

D. The Drone Industry, Research and Development

Industry is the third major actor that state drone regulations address, with an emphasis on fostering research, development and commerce. Forecasting the financial benefits that drones will have in terms of job creation, lawmakers have passed 11 bills since 2013 "to recognize the benefits of a thriving UAS industry" in their state.[77] They have also passed legislation focused on research development

---

[73] Jim Hoffer, *Small Drone Crash Lands in Manhattan*, ABC7 – EYEWITNESS NEWS - WABC (Oct. 3, 2013), abc7ny.com/archive/9270668.
[74] *Id.*
[75] *Id.*
[76] *Id.*
[77] States recognizing economic impact include: Alabama, California, Georgia, Idaho, Michigan, Nevada, and North Dakota. *See* H.R. Res. 381, Reg. Sess. (Ala. 2013); S. Con. Res. 16, 2013-14 Sess. (Cal. 2013); Assemb. J. Res. 6, 2013-14 Sess. (Cal. 2013); H.R. Res. 80, 152d Gen. Assemb., 1st Reg. Sess. (Ga. 2013); H.R. Res. 81, 152nd Gen. Assemb., 1st Reg. Sess. (Ga. 2013); S. Res. 172, 152nd Gen. Assemb., 1st Reg. Sess. (Ga. 2013); S. Con. Res. 103, 62d Legis., 1st Reg. Sess. (Idaho 2013); H.R. Res. 280, 97th Legis. (Mich. 2013); S. Con. Res. 7, 77th Sess. (Nev. 2013).

and establishing test sites.[78] For example, Hawaii's SB 661 creates a Chief Operating Officer position and advisory board to manage their drone test site.[79] Another Hawaiian bill appropriated $100,000 to the University of Hawaii to establish a training program for drone pilots.[80]

Clearly, in the absence of federal guidance, states have jumped into the fray, regulating drone operations within their borders. Lawmaker trends since the passage of the FMRA in 2012 span a wide swath of issues, from a primary focus on LEAs' potential abuse of individual privacy rights to private actor abuses in the privacy arena to encouraging RD&I.

IV. CONFLICTS OF LAWS AND NATIONAL SECURITY

A. The Current Situation

While the FAA continues to grapple with creating relevant regulations for the safe assimilation of drones into the NAS, the states already have enacted a full palette of laws. Nevertheless, when the FAA does publish their Rule governing drones within the NAS, that federal scheme will pre-empt any state laws that conflict or interfere with it. The FAA, through their OGC, has forecasted pre-emption over operational issues such as flight altitude, flight paths, operational bans, any regulation of navigable airspace, as well as mandates on equipment or training. We now turn to a review of how the previously discussed state laws and proposals would, or would not, withstand a claim of pre-emption and what the potential that such conflicts could have on national security.

[78] Test Site bills include: S.B. 661, 28th Leg. (Haw. 2015); H.R. B. 100, 2013 Reg. Sess. (Md. 2013); Assemb. B. 507, 77th Sess. (Nev. 2013); S. B. 2018, 63rd Legis. Assemb., Reg. Sess. (N.D. 2013).
[79] S.B. 661, 28th Leg. (Haw. 2015).
[80] S.B. 1221, 27th Leg. (Haw. 2013).

B. State Law Enforcement Activities

The FAA has indicated that it will defer to laws traditionally relegated to state and local police power.[81] States have enacted laws addressing a wide range of LEA-related activities, including requiring warrants before operating a drone, imposing procedural requirements associated with drone use, and allowing drone use in exigent circumstances. These types of clauses require individualized analysis and succeed based on the specific language used.

1. Warrant Requirement and Exceptions

Generally speaking, warrant requirements for state LEAs are a valid exercise of police power and would not conflict with FAA governance of the NAS; however, certain exceptions to the warrant requirement, as applied to drone operations, may conflict with federal guidance.

As an example of a law that is generally not subject to federal regulation, the FAA OCC Fact Sheet specifically enumerates, a "[r]equirement for police to obtain a warrant prior to using a UAS for surveillance."[82] Thus, the portions of Alaska House Bill 255, Florida Senate Bill 92, and Montana Senate Bill 196 that relate to search warrant requirements should withstand scrutiny.[83]

In contrast, Florida Senate Bill 92, which discusses permissible LEA drone operations without a warrant, may go too far into the operational scheme contemplated by the FAA.[84] For example, the law permits Florida LEA to use drones to pursue a fleeing felon, which may present a potential danger for flight safety in the NAS. One can imagine a scenario where a felon-pursuit leads law enforcement in a high-speed cross-border chase across the NAS. Without obedience to a consistent framework, a lack of communication could lead to operational conflict. The Supreme

---

[81] *See* FAA Fact Sheet, *supra* note 25, at 3.
[82] *Id.*
[83] H.B. 255, 28th Leg., 2d Sess. (Alaska 2014); FLA. STAT. § 934.50 (2015); S.B. 196, 63rd Leg., Reg. Sess. (Mont. 2013).
[84] FLA. STAT. § 934.50.

Court struck down a local law for less when it ruled against the City of Burbank's curfew based on aircraft noise.[85] There, the mere limiting of flight hours, which could have theoretically led to a congestion of flights in the waning hours of the day was deemed to interfere too much with the FAA's broader scheme in organizing the NAS.[86] Imagine state LEA drones racing through the skies, crossing state borders at will, in hot pursuit of a fleeing criminal. Without specific inter-state agreements or a means to rapidly dovetail into the federal air traffic control system, such dynamic LEA operations have the potential to further chaos, and danger, in the NAS.

Now imagine that the fleeing felon, a terrorist whose activities were captured by drone imagery, objects to the admissibility of the evidence based on federal pre-emption, prevails, and is exonerated . . . even though there is video of his terroristic acts. This is but one scenario that exemplifies how the potential conflict between state and federal drone legal schemes can have detrimental impacts on national security.

2. Procedural Requirements

State-imposed procedures for LEA to obtain a warrant fall within the state's police powers. For example, the provisions of Illinois Senate Bill 1587 that impose warrant waiting periods and require the protection and destruction of collected information would survive pre-emption scrutiny because they are procedural in nature and would not affect NAS operations.[87] Conversely, if a state law, like Florida Senate Bill 92, provided a procedure for launching a drone in pursuit of a fleeing felon, or a tactical communication plan with air traffic control towers, such measures would directly regulate activities in the NAS and be ripe for pre-emption.

C. Private Actors and Crime

In addition to the warrant requirement, the establishment of crimes is generally respected as within the province of local police

[85] *See* Burbank v. Lockheed Air Terminal, Inc., 411 U.S. 624, 640 (1973).
[86] *Id.* at 627, 633.
[87] S.B. 1587, 98th Gen. Assemb. (Ill. 2013).

power to govern private citizens' behavior.[88] As discussed, a number of states have moved to incorporate drone-related offenses into their criminal codes.[89] While at first blush there would seem to be no legitimate FAA interest in criminal penalties as established by a state, states may be crossing the line when they criminalize issues relevant to FAA's charter of operational safety in the NAS.

1. Drones as Aggravating Factor

On its face, crime generally falls within the purview of police power. States will likely be able to continue to enhance their criminal codes by including the use of drones in the commission of the types of offenses already codified as crimes, such as voyeurism, discussed above. Similarly, Ohio House Bill 228 enhances 23 existing crimes such as burglary, endangering aircraft, menacing, voyeurism and vandalism, among others, by creating an additional offense for engaging those activities, "through use of a drone."[90] This type of inclusion of drone offenses into a local criminal code will likely withstand federal pre-emption scrutiny, as it does not delve into the operational schema of the FAA.

2. Privacy Violations

Traditionally, the issue of privacy is also considered within state and local police power. In the instances where states are outlawing the use of drones in the commission of offenses violating privacy or private property, such laws will likely be allowed to stand. This is a logical response and extension of law that prevents a person from trespassing on one's land or from viewing someone through the window of their bordering property. As an example of this, Mississippi simply added "drones" to the list of technologically advanced devices one might use to spy on someone in private chambers, such as a periscope, telescope or binoculars.[91] Arkansas House Bill 1349 used the same approach in merely adding

[88] Randy E. Barnett, *The Proper Scope of the Police Power*, 79 NOTRE DAME L. REV. 429, 475 (2004).
[89] *See supra* notes 52-54 and accompanying text.
[90] H.B. 228, 131st Gen. Assemb., Reg. Sess. (Ohio 2015).
[91] S.B. 2022, 2015. Leg., Reg. Sess. (Miss. 2015).

"unmanned vehicle or aircraft" as another way in which the crime of voyeurism could be committed.[92]

3. Real Property and Trespass

Similarly, trespass is an offense upon real property, a prerogative of the states. Texas House Bill 1481 ("H.B. 1481"), passed into law in 2015, bans the use of drones over critical infrastructure.[93] As noted above, pursuant to the City of Burbank case, federal courts closely scrutinize state and local regulation of overflight.[94] However, the definition of "critical infrastructure" in H.B. 1481 makes it more akin to a criminal trespass statute than a regulation on flight paths. It describes such infrastructure as:

> completely enclosed by a fence or other physical barrier that is obviously designed to exclude intruders, or if clearly marked with a sign or signs that are posted on the property, are reasonably likely to come to the attention of intruders, and indicate that entry is forbidden.[95]

Like the voyeurism statutes discussed above, H.B. 1481 merely adds drones as a means by which a trespass is accomplished. It further clarifies that an offense is committed when a person:

> (1) operates an unmanned aircraft over a critical infrastructure facility and the unmanned aircraft is not higher than 400 feet above ground level;
>
> (2) allows an unmanned aircraft to make contact with a critical infrastructure facility, including any person or object on the premises of or within the facility; or
>
> (3) allows an unmanned aircraft to come within a distance of a critical infrastructure facility that is close enough to interfere with the operations of or cause a disturbance to the facility.[96]

---

[92] H.B. 1349, 90th Gen. Assemb., Reg. Sess. (Ark. 2015).
[93] H.B. 1481, 84th Leg., Reg. Sess. (Tex. 2015).
[94] *See* FAA Fact Sheet, *supra* note 25, at 3.
[95] H.B. 1481, 83rd Reg. Sess. (Tex. 2015).
[96] *Id.* (amending Tex. Gov. Code by adding § 423.0045(b)).

By focusing on drone flights under 400 feet, subparagraph 1 clearly establishes that the offense is not about a flight path under the purview of the FAA. Furthermore, subparagraphs 2 and 3 continue to hone in on trespass and interference with property as the primary purpose of the law. Therefore, H.B. 1481 and others like it should survive federal pre-emption challenge because the establishment of such a crime is a central function of state police power.

There is a fine line for a state to walk between treating drone incursions as trespass and creating a pre-empted ban in navigable airspace. This is why it is critical that any FAA drone scheme address states' concerns and incorporate them into plans for geo-fences or no-drone zones. Local governments and agencies should reach out to the FAA to incorporate their concerns concerning landmarks, significant infrastructure and large public gathering facilities. These types of locations are of great national security interest and without a consistent framework establishing restrictions on drone use around them, vulnerabilities will persist.

4. Broad Discretionary Crimes

In contrast to the few examples outlined relating to warrant requirements, criminalization of private actors' behavior and protection of privacy and real property, states may overstep their boundaries by broadly reserving the right to criminalize drone flights over their land. North Carolina Senate Bill 744, which proclaims that the state will determine whether any action by a drone pilot flying over the state is a crime, is an example of this.[97] While nothing about this general provision in and of itself is ripe for pre-emption, North Carolina could find itself in the pre-emption crosshairs if it decides to criminalize a drone activity that is not within the typical police powers of the state or obstructs the FAA scheme.

5. Penalties for Training and Certification Violations

In its Fact Sheet, the FAA OCC noted, "[m]andating equipment or training for UAS related to aviation safety such as geo-

[97] S.B. 744, 2013 Gen. Assemb., Reg. Sess. (N.C. 2013).

fencing would likely be pre-empted."[98] Thus, if any State were to require a particular training and make the failure to accomplish a crime, even a low-class misdemeanor, such a crime could be pre-empted as interfering with the FAA Rule.

6. Hunting Restrictions

Five state laws thus far criminalize the use of privately operated drones in hunting or to interfere with hunting.[99] The regulation of hunting and fishing is traditionally left to the states, a concept respected by the FAA.[100]

Not surprisingly, these state laws address the issue of arming a drone for the purposes of hunting. However, the weaponization of drones, even if for hunting, is also a national security concern. While hunting may be within the traditional domain of the states, the FAA is charged with the efficient organization and safe use of the NAS consistent with national security. The mere possibility of a drone "flyaway" while armed is alarming.[101] For example, the pilot of the drone that landed on the White House lawn claimed that his incident was the result of such a flyaway.[102] What if it had been armed for hunting and taken off just across the Potomac in Virginia before suffering a flyaway malfunction?

The malfunction of a drone while armed for hunting is one of the most benign scenarios one could posit. Anyone with malicious intentions could rig a drone to exact devastating loss of life

---

[98] *See* FAA Fact Sheet, *supra* note 25, at 3; Air Evac EMS, Inc. v. Robinson, 486 F. Supp. 2d 713, 722 (M.D. Tenn. 2007).

[99] *See* FAA Fact Sheet, *supra* note 25, at 3; *Current Unmanned Aircraft State Law Landscape,* NAT'L CONF. OF STATE LAW LEGISLATURES (Apr. 6, 2016), http://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx.

[100] *See* FAA Fact Sheet, *supra* note 25, at 3 (examples of State and Local Laws within State and Local Government Police Power).

[101] Jack Nicas, *What Happens When Your Drone Escapes*, WALL ST. J. (Dec. 8, 2014, 7:51 PM), http://www. wsj.com/articles/what-happens-when-your-drone-escapes-1418086281.

[102] Jim Acosta & Pamela Brown, *First on CNN: No Charges Against White House Drone Flyer*, CNN (March 18, 2015), http://www.cnn.com/2015/03/18/politics/white-house-drone-charges/.

and terror with any of the commercially available drones capable of carrying a significant firearm, explosive, chemical, or biological payload. It is easily within the domain of the FAA's mandate to ban the arming of drones for any use, trumping any state law regulating permissible armed drone hunting. Despite the FAA OCC position on this issue, weaponization of drones is clearly an area with broad national security interest that cannot be handled by the States individually, and needs to be addressed at the federal level by the FAA.

D. The Drone Industry, Research and Development

Pursuant to the mandate in the FMRA, the FAA set out to establish six drone test sites run by non-federal public agencies to accelerate the integration of drones into the NAS. Programs were solicited and selected by the FAA Administrator.[103] The six sites selected were: Griffiss International Airport, North Dakota Department of Commerce, the State of Nevada, Texas A&M University-Corpus Christi, University of Alaska; and Virginia Polytechnic Institute and State University. Their programs span across 20 different test locations in 14 states, all of which have legislated to authorize and fund them, as necessary.[104] While these particular laws fall squarely within the FAA's mandate to establish research programs to assist in integrating drones into the NAS, if any other state were to establish a similar test site, such would be pre-empted by the FAA Administrator's Order.[105] Specifically because some of the additional factors considered for site selection were "sites where UAS can be safely and efficiently" tested for integration into the NAS, it could be presumed that anything outside FAA-approved sites could be presumed to interfere with the NAS.

Also related to industry, manufacturing specifications for the drone industry would also likely not survive a pre-emption challenge.

---

[103] *See* U.S. DEP'T OF TRANSP., FAA, SELECTION OF SIX UNMANNED AIRCRAFT SYSTEMS TEST SITES IN ACCORDANCE WITH FAA MODERNIZATION AND REFORM ACT OF 2012, PL-112-95 (Dec. 30, 2013); *see also Test Sites*, U.S. DEP'T OF TRANSP., FAA, http://www.faa.gov/uas/legislative_programs/test_sites/ (last modified Aug. 4, 2015).
[104] *See* U.S. DEP'T OF TRANSP., *supra* note 103; FAA Fact Sheet, *supra* note 25, at 3.
[105] *See* U.S. DEP'T OF TRANSP., *supra* note 103.

For example, in the aftermath of the White House lawn incident, drone-builder DJI voluntarily patched and sent out an update to its drone software, putting a geo-fence around the entire downtown Washington D.C. area.[106] Imagine the impacts upon drone manufacturers if every state produced its own geo-fencing requirements. Conceivably, the FAA will claim dominion over any future directives regarding geo-fences protecting areas of national priority.[107] The centralization of this process in the FAA will likely be to the benefit of manufacturers who will have to look to one regulatory agency instead of 50, governing what safety mechanisms they must install in a drone.

E. Absence of National Regulatory Scheme as National Security Threat

The patchwork of state drone laws, discussed above, spawned in response to FAA inaction. While it is generally true that technology will usually outpace the law, the explosion of drone technology available to the public not only presents unique legal challenges, it also creates real practical dangers. If one looks at the FAA definition of an aircraft, which includes both airplanes and drones,[108] it is troubling that over the last few years, thousands of new aircraft are populating the skies, flown by unlicensed, untrained, and minimally regulated pilots. Some may want to dismiss this concern and say these drones are just toys or will be used responsibly by industry. However, as discussed, these small non-traditional aircraft have the capacity, intentionally or not, to create devastation.[109]

The unintentional threat is characterized by operational safety hazards posed by the average American flying a drone. Drone proliferation has made it possible for anyone to launch a resilient

---

[106] *DJI has Released the New Rirmware v3.12 for Phantom 2 Series Quadcopter*, DJI, http://www.dji.com/newsroom/news/dji-has-released-the-new-firmware-v3-12-for-phantom-2-series-quadcopter (last visited Apr. 10, 2016).

[107] *See* Press Release, FAA, FAA Selects Unmanned Aircraft Systems Research and Test Sites (Dec. 30, 2013), http://www.faa.gov/news/press_releases/news_story.cfm?newsid=15576.

[108] 14 C.F.R. 1.1 (2015).

[109] *See* INTRODUCTION, *supra*.

plastic and metal machine into the sky. Without a national operational framework and associated education campaign, the average person likely has no idea about the restrictions or requirements imposed by their own state and local governments, let alone those of neighboring jurisdictions. Other unintentional threats include drones that could have flyaway malfunctions.

The greater national security concern, however, lies with the incohesive regulatory framework to respond to this diffuse capability to deliver a destructive payload remotely by air. Since the end of WWII, the United States has maintained a strategic advantage worldwide due to its air superiority defined by a premier lineup of traditional combat aircraft: support, intelligence, attack, and bomber.[110] Drones present a macro-security problem due to their micro-size coupled with their strategic advantage from the sky. One does not have to strain to imagine scenarios where the lack of organized regulation has created vulnerabilities. For instance, while there have been prohibitions against flying drones around sports stadiums (e.g., the Super Bowl),[111] not all mass gatherings have such legal or policy protection. Even if they did, what plans are in place in the event of an attack? Take the following scenario: a drone flies over a community 5K run and starts dropping a white powdery substance. Here are just a few of the questions that must be considered:

- Who is responsible to take action? Local, state, or Federal?
- Are those various levels of government agencies prepared to collaborate?
- What is the substance?
- Might it also be carrying an explosive?

---

[110] *See Challenges and Capabilities of the U.S. Air Force*, USAF (Feb. 9, 2005), http://www.af.mil/AboutUs/SpeechesArchive/Display/tabid/268/Article/143991/challenges-and-capabilities-of-the-us-air-force.aspx (remarks at the 2005 Air Force Defense Strategy and Transformation Seminar Series, Washington DC).

[111] A huge public gathering, Super Bowl 50 garnered more than just a drone no-fly zone around the stadium. Rather, the FAA banned the entire 32-mile radius surrounding Levi Stadium. *See* James Eng, *FAA: Drones Flown Around the Super Bowl Could Face 'Deadly Force'*, NBC NEWS (Feb. 3, 2016), http://www.nbcnews.com/storyline/super-bowl/faa-drones-flown-around-super-bowl-could-face-deadly-force-n510606.

- Where is the remote pilot?
- Should we send up an armed police drone to shoot it down?
- Can we shoot it down from the ground?
- Could we jam the remote signal?
- Can authorities identify the aggressor drone vs. friendly drones?
- Can authorities identify friendly support from another jurisdiction?

Answers to these factual questions are difficult enough in such a hypothetical situation. However, the procedural questions also remain unanswered by the current regulatory and policy landscape. The United States lacks a framework to guide the decision-making process in such an event. The FAA may have been tracking security at Super Bowl 50, but they are not covering the mid-sized city Fun Run or the summer concert series at the community park. Federal authorities are not monitoring lunch hour in downtown Chicago, standing by and waiting to respond to a drone threat. The responsibility to respond to incidents under these circumstances is less clear, and therein lies the crux of the problem. Emergencies, particularly terrorist events, are inherently chaotic. Without proper organization to restore order, haphazard government actions are likely to add more confusion to the situation and potentially cause more harm. If every state is left to figure this out, the potential patchwork quilt of regulations on warrants, information collection, no-fly zones, hunting drones, manufacturer requirements, and more, would greatly inhibit a coordinated response to a disaster. Only a national regulatory framework as dictated by the FAA can resolve such discrepancies. At the very least, a federal delegation of responsibilities to state and local governments with specific guidelines for cooperation would be a step in the right direction.

V. CONCLUSION

In stark contrast to the rate of speed at which the drone industry has accelerated, the law has failed to keep pace. The current legal landscape applicable to domestic drone use is a patchwork of

seemingly random state rules that sometimes conflict with current and proposed federal guidance and fail to address issues crucial to our national security.

Because the FAA continues to struggle with how to best balance safety requirements with operational flexibility, a final rule for small commercial drones remains elusive. In the meantime, to bridge the regulatory gap, individual states have created a host of laws regulating drone activities in the skies above their land targeting governmental, private and commercial actors' drone use across a wide range of issues. From trespass in relation to critical infrastructure, to drones-as-hunting weapon bans, to restrictions against potential Fourth Amendment violations by law enforcement, inconsistency prevails.

Such legal ambiguity, especially when viewed through the lens of pre-emption, can lead to intentional and unintentional consequences. Nefarious actors continue to have room to maneuver with relative impunity and with potential amnesty from prosecution. The resultant environment, as illustrated by the fleeing felon drone chase across borders, is also ripe for accident.

A comprehensive national federal framework for domestic drone use is required. Such a framework must address not only safety, but also security. The states should regulate privacy, property and crimes, as they relate to drone operations above their land. They should do so in consultation with the FAA so as not to contravene FAA's field of regulation. However, the FAA remains in the best position to promulgate safety and security rules consistent with their already established requirements for manned aircraft, with special consideration given for the unique attributes of unmanned flight. Failure to do so, in the wake of the democratization of airpower to individual users, is, in and of itself, a threat to our national security.

APPENDIX A

State Legislation Enacted by Topic

Total Bills:	70
State Bills:	69
Governor Initiated:	1
Law Enforcement Focused Bills:	25
Private Actor Focused Bills:	19
Hunting Bills:	5
Test Site Establishment:	5
Recognition of Industry Benefits:	11
L.E. Must Obtain Warrant:	17
Exigent Circumstances:	3
Consent Exception:	6
Amber/Missing Person Alerts:	5
Terror Threat Exception:	6
Critical Infrastructure Protection:	1
Felony Penalty:	5
Misdemeanor Penalty:	6
Civil Penalties:	7
Voyeurism Prohibited:	2

ASCULUM DEFEATS:
PROSECUTORIAL LOSSES IN THE MILITARY COMMISSIONS AND HOW THEY HELP THE UNITED STATES

John M. Bickers*

Small but consistent failures have marked the U.S. endeavor to use military commissions in the struggle against Al Qaeda. The handful of cases have mostly ended in reversals of convictions and sentences. This article will consider the possibility that conflating two kinds of crimes created the legal errors that led to these defeats. Law of war military commissions have historically been used not only as extraordinary venues for prominent war criminals, but also for preserving the vital role of combatant immunity. Commissions thus tried those accused of grave breaches of international law as well as the kind of ordinary belligerency offenses that would not even have been illegal had the perpetrators been legitimate combatants. Because the military commissions stemming from the War on Terror drew precedent from all manner of past military commissions, whose rules contemplated trials for both kinds of accused, the government wandered into an ever-more labyrinthine view of the law appropriate to the commissions. The article will consider the completed cases, focusing on the prosecution's choice to emphasize inchoate offenses. It will then compare international and domestic law and suggest that the government's losses occurred because of the inappropriate amalgamation of grave breaches and belligerency offenses, and that the assessment of liability is very different between the two.

International law has long recognized some species of expansive liability for grave breaches, but not for belligerency offenses. Because

*Professor, Salmon P. Chase College of Law, Northern Kentucky University. My great thanks to research assistant Sarah C. Larcade, my colleagues of the Central States Law Schools Association and the Chase College of Law, who gave me invaluable feedback for earlier versions of these paper, and William Aceves, who provided help with the final version.

most detainee trials to date have been for belligerency offenses, the reliance on offenses like conspiracy and material support for terrorism has led to a string of reversals. This article will suggest, however, that these defeats suffered by the United States have actually been to its benefit. In the short term, the loss of confidence in the military commissions might make possible a federal trial for some of the remaining detainees, such as Khalid Shaikh Mohammed. The world benefits from a public trial of persons accused of grave breaches, but a U.S. military commission can no longer realize most of that potential benefit. In the long term, a regime of international law that provided expanded liability for belligerency offenses would greatly harm U.S. strategic interests. By losing a series of small judicial battles, the United States is positioned to win a much more significant war.

INTRODUCTION

"Pyrrhus replied to one that gave him joy of his victory that one other such would utterly undo him."[1]

The victory of King Pyrrhus of Epirus over the Romans[2] is such a well-known feature of modern Western culture that it has become its own trope for movies,[3] television,[4] and books.[5] After the battle at Asculum, Plutarch reports the quote above as Pyrrhus's morose response to the good news. Pyrrhus clearly recognized that his victory was so costly that the tactical advantage he gained was not truly worth the strategic loss he had suffered.[6] Such a "Pyrrhic victory" offers an oddly counterintuitive lesson: winning is, in such a case, only the precursor to ultimate loss. King Pyrrhus, and his struggle for Hellenic dominance in the Mediterranean, would have been much better off had he never fought the battle. His brief successes led to the failures that enabled Rome to conquer all of Italy.[7]

Seldom do we notice the other side of the equation. The Romans, this suggests, were better off for having fought and lost this battle. Had Pyrrhus husbanded his forces, he might have frustrated Roman plans much longer.[8] In the long term, the Romans benefitted

---

[1] PLUTARCH, THE LIVES OF THE NOBLE GRECIANS AND ROMANS 483 (JOHN DRYDEN TRANS., MODERN LIBRARY 1932).

[2] *Id.*

[3] *See, e.g.,* Randall King, *Cruise Control: Star's Presence Overpowers What Could Be a Smart Science-fiction Story,* WINNIPEG FREE PRESS (Apr. 19, 2013) (characterizing Earth's victory over an alien enemy in "Oblivion" as Pyrrhic); Shea Conner, *Movie Review: 'Lincoln'*, ST. JOSEPH NEWS-PRESS (Nov. 8, 2012) (noting that winning the civil war before passage of the Thirteenth Amendment could have proved a Pyrrhic victory for the cause of emancipation).

[4] *See, e.g.,* Sarah Rodman, *Buckle Up for Wild Ride to the Bottom,* BOSTON GLOBE (July 13, 2012) (describing the opening of the final season of *Breaking Bad* as such a victory); Paul Brownfield, *Jump Back In*, LA TIMES (Apr. 3, 2007) (describing the victories of Tony in The Sopranos as Pyrrhic).

[5] *See, e.g.*, WALLACE THURMAN, THE BLACKER THE BERRY (1929).

[6] PLUTARCH, *supra* note 1, at 483.

[7] *Id.* at 486.

[8] Plutarch gives some credit both to Roman sacrificial auguries and the retreat of the elephants of Pyrrhus at the subsequent battle of Beneventum. *Id.*

from a loss that they certainly did not greet with joy: like Voltaire's Zadig,[9] they had no idea at the time how beneficial the loss would become.

Similarly, the United States appears to have suffered a number of legal defeats in the effort to conduct trials by military commission. Like the Romans at Asculum, though, those very defeats may actually have benefitted the very government that lost them.

Since the attacks of September 11, 2001, the U.S. Government has faced a series of difficult legal choices about how to detain, and possibly punish, members of the forces opposing it. One early decision resurrected the system of military commissions not seen in American law since the aftermath of the Second World War.[10] An accompanying decision transformed the U.S. Naval Base at Guantanamo Bay, Cuba, into a detention center for foreign citizens who came into the custody of U.S. forces.[11] A third decision linked these two choices, establishing Guantanamo as the venue for any trials by military commission that the War on Terror brought forth.[12] Each of these choices has generated huge scholarly output,[13]

[9] The titular protagonist of Voltaire's story is a Babylonian philosopher who is instructed by an angel disguised as a hermit. The angel teaches Zadig that deeds that appear to be bad may turn out later to be good, and vice versa. VOLTAIRE, CANDIDE & SELECTED STORIES 169 (Donald M. Frame, trans., The New American Library 1961) ("'Men,' said the angel Jesrad, 'pass judgment on everything without knowing anything.'").

[10] Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terrorism, 66 Fed. Reg. 57,831 (Nov. 16, 2001).

[11] Janet Cooper Alexander, *The Law-Free Zone and Back Again*, 2013 U. ILL. L. REV. 551, 557 (2013).

[12] Janet Cooper Alexander, *Military Commissions: A Place Outside the Law's Reach*, 56 ST. LOUIS U. L. J. 1115, 1118 (2012).

[13] *See, e.g.*, Gerald Neuman, *Extraterritoriality and the Interest of the United States in Regulating Its Own,* 99 CORNELL L. REV. 1441, 1459 (2014); David Glazier, *Destined for an Epic Fail: The Problematic Guantanamo Military Commissions*, 75 OHIO ST. L. J. 903, 915 (2014). *See generally* Aziz Z. Huq, *Forum Choice for Terrorism Suspects,* 61 DUKE L. J. 1415 (2012); Gabor Rona, *Legal Issues in the "War on Terrorism" - Reflecting on the Conversation between Silja N.U. Voneky and John Bellinger*, 9 GERMAN L.J. 711 (2008); David Frakt, *The Practice of Criminal Law in the Guantánamo Military Commissions*, 67 A.F. L. REV. 35 (2011); Peter Margulies, *Defining, Punishing, and Membership in the Community of Nations: Material*

along with many judicial challenges in various fora.[14] Neither the Bush nor Obama Administrations have had consistent winning streaks while defending these decisions. Both suffered rebukes from courts that required them to redesign their legal plans repeatedly by enlisting the help of Congress.[15] Even after congressional assistance, more defeats ensued.

This article reviews some of those defeats, as well as some of the relatively easy victories that accompanied them. Part I considers the possibility that conflating two kinds of crimes in commissions contributed to a recurrence of legal errors that called forth judicial upbraiding. Military commissions have multiple roles, and the United States has historically used them not only as extraordinary venues for prominent leaders accused of war crimes, but also for much more ordinary soldiers and other belligerents.[16] Small but consistent failures have resulted from the government's attempts to resolve cases involving both kinds of accused persons under commissions, resulting in an ever-more labyrinthine view of the appropriate law to apply to modern commissions. Part II examines the handful of cases completed since the beginning of the War on Terror, looking to the differences between those that ended with successful convictions, and those that the defendant successfully appealed. Part III, which looks to the reason for the failures, concludes that the die was cast by the government's insistent reliance on charges of inchoate conspiracy and material support for terrorism. Part III will then compare international and domestic law and suggest that the government's losses occurred because of the conflation of grave breaches and belligerency offenses, and that the

Support and Conspiracy Charges in Military Commissions, 36 FORDHAM INT'L L.J. 1 (2013); Geoffrey S. Corn & Chris Jenks, *A Military Justice Solution in Search of a Problem: A Response to Vladeck*,104 GEO. L.J. ONLINE 29 (2015).

[14] *See infra* at Part II.

[15] *See, e.g.*, the Detainee Treatment Act, Pub. L. No. 109-148, div. A, tit. X, 119 Stat. 2680, 2739-44 (2005) [hereinafter D.T.A.], and the Military Commissions Act of 2006, Pub. L. No. 109-366, 120 Stat. 2600 (2006) [hereinafter M.C.A.].

[16] *Compare* Application of Yamashita, 327 U.S. 1, 14 (1946) (wherein the charge alleged the execution of a plan by which "more than 25,000 men, women and children, all unarmed noncombatant civilians, were brutally mistreated and killed"), *with Ex Parte* Quirin, 317 U.S. 1, 7-8 (1942) (the accused possessed explosives with the intent to "to destroy war industries and war facilities in the United States").

treatment of liability for inchoate offenses is very different between the two. Lastly, Part IV will suggest that these setbacks suffered by the United States have actually been to its benefit. In the short term, the loss of confidence in the military commissions might make possible a federal trial for some of the remaining detainees, such as Khalid Shaikh Mohammed. The nation and the world benefit from a public trial of persons accused of grave breaches, but most of that potential gain can no longer be realized by a U.S. military commission. In the long term, a regime of international law that provided expanded liability for belligerency offenses would greatly harm U.S. strategic interests. Had the United States gotten what it wanted, it would have regretted it in both the near and long term future. Instead, the United States, like Rome before it, has benefitted from a series of Asculum defeats.

I. BY ANY OTHER NAME: CONFLATING THE CRIMES TRIED BY COMMISSIONS

A. Overview of Commissions

The Supreme Court has recognized three distinct types of military commissions.[17] Two of them, martial law and military government commissions, function in place of ordinary criminal law courts when those are not available.[18] The third, law of war commissions, are defined not by their location but by their jurisdiction.[19] Martial law commissions occur domestically when a breakdown in order or threat of invasion has led to a declaration of martial law.[20] Military government commissions happen on foreign soil, when occupation by the United States requires the use of commissions to keep law and order in the absence of a local government.[21] Martial law was never at issue in the U.S. war against

[17] Hamdan v. Rumsfeld, 548 U.S. 557, 595-97 (2006) (plurality opinion).
[18] *Id.*
[19] *Id.*
[20] The Supreme Court has established limits on such commissions. *Id.* at 595*; see* Duncan v. Kahanamoku, 327 U.S. 304, 324 (1946) (holding that a statute authorizing martial law does not "authorize the supplanting of courts by military tribunals").
[21] Hamdan, 548 U.S. at 595-96.

Al Qaeda.[22] The attacks of September 11, 2001, though horrific, were not accompanied by a legitimate fear of invasion by enemy forces.[23]

Likewise, the United States does not appear to have seriously considered using military commissions as an arm of military governance. This reluctance may stem from the United States obligation to maintain local courts, even as an occupying force.[24] Using military commissions to enforce ordinary criminal laws against larceny of private property, or even murder,[25] was once a commonplace of international conduct.[26] Although the precedents have not been formally displaced, the development of a large body of law governing occupations has largely discouraged such methods.[27] Further, a global rejection of the very concept of occupation has fostered a desire among many countries to create local autonomy

[22] Glazier, *supra* note 13, at 912.
[23] Duncan, 327 U.S. at 324 (court's holding in Duncan only allows military commissions where civilian courts do not function, they were never an option after Al Qaeda's attack).
[24] *See* YORAM DINSTEIN, THE INTERNATIONAL LAW OF BELLIGERENT OCCUPATION, 132 (2009).
[25] *See, e.g.*, Madsen v. Kinsella, 343 U.S. 341 (1952) (holding that a U.S. military commissions in post-World War II Germany had jurisdiction to try for murder the civilian wife of an American military officer because the commission was "designed especially to meet the needs of law enforcement in that occupied territory in relation to civilians and to nonmilitary offenses").
[26] *See* Michael O. Lacey, *Military Commissions: A Historical Survey*, 2002 ARMY LAW 41, 41-42 (2002) (the earliest uses of military tribunals tended to be for what we would now characterize as law of war offenses, such as those convened by King Gustavus Adolphus during the Thirty Years War and nations have used them for hundreds of years for general matters of governance). *See* Anil Kalhan, et al., *Colonial Continuities: Human Rights, Terrorism, and Security Laws in India*, 20 COLUM. J. ASIAN L. 93, 126 (2006) (noting that an act of 1861 granted the Governor-General authorization to convene "special tribunals" to preserve law and order); PETER JUDSON RICHARDS, EXTRAORDINARY JUSTICE: MILITARY TRIBUNALS IN HISTORICAL AND INTERNATIONAL CONTEXT, 18-19 (2007) (noting that Winfield Scott's General Order creating such military commissions primarily "identified criminal offenses normally cognizable by civil courts in time of peace"); *id.* at 73-74 (noting that French principles of republicanism limited the use of such tribunals, *les conseils de guerre*, to "the state of siege").
[27] *See, e.g.*, Conference of High Contracting Parties to the Fourth Geneva Convention, Geneva, Switz., Aug. 12, 1949 (Feb. 2, 1956) 6 U.S.T. 3516.

over such matters,[28] even before a formal transfer of authority to the host nation which may be more formal than real.

Thus, although the current commissions have been of the law of war variety,[29] the existence of precedents of all three kinds has led to confusion about their jurisdiction.[30] That confusion was evident in the recent argument among federal judges about the nature of the commissions that tried those accused of conspiring in the plot to kill President Lincoln and other senior government officials in April 1865.[31] Whether conspiracy was actually triable by military commissions divided a panel of the U.S. Court of Appeals for the D.C. Circuit ("D.C. Circuit").[32] Part of the reason for the split was a disagreement over whether the Lincoln commissions furnished valid precedent as a law of war commission, or whether their value must be discounted because they were mixed commissions, functioning in both the law of war and martial law realms.[33]

B. Distinguishing Conduct in War

Confusion has resulted in the area of subject-matter jurisdiction. The terms "war crime" or "violation of the law of armed conflict" have been used interchangeably to describe two very

[28] "After WWII - possibly due to the odium attached to belligerent occupation by the appalling Nazi and Japanese record - there has been a considerable reluctance by States to admit that they were Occupying Powers." DINSTEIN, *supra* note 24, at 10. There are also sound practical reasons that promote a devolution of power, "the military government of an occupied territory would be eager to avail itself of the continued service of some low-level officials....The reason is prosaic: it is a matter of expediency and conservation of resources." *Id.* at 57.

[29] *See* Hamdan v. Rumsfeld, 548 U.S. 557, 597 (2006) ("Since Guantanamo Bay is neither enemy-occupied territory nor under martial law, the law-of-war commission is the only model available.").

[30] *See, e.g.*, Al Bahlul v. United States, 792 F.3d 1 (D.C. Cir. 2015).

[31] WILLIAM H. REHNQUIST, ALL THE LAWS BUT ONE: CIVIL LIBERTIES IN WARTIME 145 (Nancy Spears & Patricia Hass eds., 1st ed. 1998).

[32] *See generally* Al Bahlul v. United States, 792 F.3d 1 (D.C. Cir. 2015).

[33] *Compare Al Bahlul*, 792 F.3d at 12 ("Winthrop noted that the Lincoln assassins' tribunal was a mixed martial law and law of war military commission"), *with id.* at 60 (Henderson, J., dissenting) ("because the military cannot exercise martial law jurisdiction unless civilian courts are closed (citation omitted), the Lincoln conspirators' military court necessarily was purely a military commission with law-of-war (including conspiracy) jurisdiction").

different types of offenses against international order: grave breaches and belligerency offenses.[34] International and domestic law of war commissions have tried both of these two species of crime.[35] Therefore, the precedents have a surface similarity. Unfortunately, because of their fundamentally different natures, these two varieties of crime have completely separate rules regarding liability for inchoate offenses such as conspiracy.[36] Because courts have often merged these two strands similarly, they have at times erred by applying the conclusions from one area of law to the other.[37] What this article will call "belligerency offenses" are those acts that represent the ordinary duties of military forces, when committed by those who are not part of a legitimate military force. Soldiers and sailors function by destroying the fighting capacity of their enemy: in short, by harming people and things. The primary mission of an armed force, the reduction of opposing military forces, by definition requires the killing and wounding of humans and the destruction of

[34] *Compare Ex parte* Quirin, 317 U.S. 1, 14 n.12 (1942) ("Authorities on International Law have regarded as war criminals such persons who pass through the lines for the purpose of (a) destroying bridges, war materials, communication facilities etc."), *with* DINSTEIN, *supra* note 24, at 95 ("It is for the Occupying Power to determine—through legislation—what specific acts…constitute punishable acts of sabotage when committed in occupied territory. International law, as such, does not penalize these acts").

[35] Some scholars use the phrase "direct participation in hostilities" for the same species of offense. *See, e.g.,* David Frakt, *Direct Participation in Hostilities as a War Crime: America's Failed Efforts to Change the Law of War*, 46 VAL. U.L. REV. 729, 752 (2012). Because it is difficult to characterize many of the acts the United States has attempted to punish at the military commissions as "direct participation," I have opted for the more general "belligerency offenses."

[36] *See, e.g.,* Allison Marson Danner & Jenny S. Martinez, *Guilty Associations: Joint Criminal Enterprise, Command Responsibility, and the Development of International Criminal Law,* 93 CAL. L. REV. 75, 118 (2005) (noting the differences between joint criminal enterprise under international law and the common law doctrine of conspiracy).

[37] This was the source of the dispute between the majority and dissent in the al Bahlul case: if the tribunal that tried the Lincoln conspirators were of the same type as the commission faced by al Bahlul, it stood as precedent for the use of conspiracy. If it was a different type, it could not do so. *See Al Bahlul*, 792 F.3d at 12.

property.[38] Such acts, outside of the context of war, are generally the subject of criminal sanction.[39]

This concept of "combatant immunity" arose from an ancient recognition that punishing an enemy soldier for those ordinary military acts would significantly decrease the willingness of enemies to surrender or otherwise cease fighting.[40] A desire to avoid a perpetual state of war required battlefield forces to accept that their surrender was not a death sentence. Because of this very realistic assessment of human nature, the notion that enemy soldiers had not committed murder is one of the oldest principles of the law of war.[41] Only those countries and regimes that deliberately sought to escalate conflicts into existential struggles violated it.[42]

Because this immunity meant that the military was treated differently in terms of criminal liability, it became important to determine who qualified for this different treatment. An area of

[38] This is so central a concept that the classical legal documents governing armed conflict treated it as the most basic underlying assumption. *See* Hague Convention No. IV Respecting the Laws and Customs of War on Land, 36 Stat. 2259, Art. 22 (1907) ("The right of belligerents to adopt means of injuring the enemy is not unlimited").

[39] Glazier, *supra* note 13, at 915 ("All societies criminalize deliberate killing and destruction of property, the very acts that governments require their militaries to perform during war").

[40] This idea is an old one indeed, and is suggested even by ancient China's great military philosopher. *See* SUN TZU, THE ART OF WAR 76 (Samuel B. Griffith, trans., Oxford University Press, 1963) ("Treat the captives well, and care for them...This is called 'winning a battle and becoming stronger'").

[41] Thus, punishing them as if they had committed murder is itself wrong. In his otherwise hagiographic play about Henry V, Shakespeare allows a Welsh officer to criticize King Henry V for ordering the killing of prisoners of war. WILLIAM SHAKESPEARE, THE LIFE OF HENRY THE FIFTH act 4, sc. 7 ("Kill the poys and the luggage! 'tis expressly against the law of arms: 'tis as arrant a piece of knavery, mark you now, as can be offer't, in your conscience, now, is it not?").

[42] Richard J. Galvin, *The Case for a Japanese Truth Commission Covering World War II Era Japanese War Crimes*, 11 TUL. J. INT'L & COMP. L. 59, 69 (2003) (describing the Imperial conviction that prisoners of war were essentially military supplies to be used as needed and observing that "Japanese administrative personnel in the Burma-Thailand camps further conveyed their philosophy through arm bands, which stated: 'One captured in battle is to be beheaded and castrated at the will of the Emperor'").

great development over the last two centuries has concerned this very issue.[43] Some people and nations sought to expand the definition of combatant immunity, and others sought to maintain a narrow definition.[44] Belligerency offenses, then, are those acts that would not be criminal if committed by those who possessed this immunity.[45] Otherwise conforming to the law of war, such acts would be the ordinary duties of an ordinary soldier. Only if a civilian committed them, someone who did not qualify as a soldier, would they become punishable.[46]

This article will use the term "grave breaches," on the other hand, for those offenses that violate such fundamental tenets of international law that it does not matter if the individuals who committed them were soldiers or civilians.[47] The globalization and mechanization of warfare in the 20th century led to an increasing reliance on national behavior that shocked and frightened much of humanity.[48] World War II in particular saw massive attacks on

[43] Because there had been centuries of custom in the development of the law of war, the earliest work at setting the rules down in conventions acknowledged, in the famous Maartens clause, that such customs provided a basis for the protection of both soldiers and civilians. Rona, *supra* note 13, at 714.

[44] A series of revolutions against colonial governance were largely responsible for the extraordinary transition of this area in three decades, from the carefully detailed list of qualifications for combatant status of 1949, to the much broader approach taken by the 1977 Protocol. *See* Geneva Convention Relative to the Treatment of Prisoners of War, art. 4, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), art. 44, June 8, 1977, 1125 U.N.T.S. 3 (allowing combatants to maintain their status providing only that they carry arms openly while fighting, and while "visible to the adversary while he is engaged in a military deployment preceding the launching of an attack . . . .").

[45] *See* Derek Jinks, *The Declining Significance of POW Status*, 45 HARV. INT'L L. J. 367, 436-38 (2004).

[46] *See id.*

[47] GARY D. SOLIS, THE LAW OF ARMED CONFLICT: INTERNATIONAL HUMANITARIAN LAW IN WAR, 309-10 (2010) (citing the post-World War II trial of the manufacturers of the poison gas used in Nazi death camps).

[48] *See, e.g.*, ARCHER JONES, THE ART OF WAR IN THE WESTERN WORLD 579 (2001) (describing a primary facet of strategic bombing in World War II as "compelling the enemy to end the war through the terror of the raids").

civilian populations, both within and outside the jurisdiction of occupying powers.[49]

The sense of "never again"[50] that led to the convening of the International Military Tribunal at Nuremberg [51] inspired the gathering in Geneva to rewrite and reform humanitarian law.[52] The four Conventions produced there, and now agreed to by every nation on the earth,[53] set forth a series of "grave breaches," offenses so terrible that subscribing parties to the conventions have an affirmative duty to prevent and punish them.[54] The commission of these offenses may lead to criminal penalties regardless of the actor's status.[55] Legitimate military service is simply not relevant in a determination of guilt: being a soldier will not prevent a conviction, nor will being a civilian.[56] Although the list of grave breaches in the Geneva Conventions seems quite limited, this article will use the

[49] *See* THEODORE ROPP, WAR IN THE MODERN WORLD 380 (1959) (noting the hundreds of thousands killed by the atomic bombs dropped on Japan at the end of World War II, and quoting U.S. General H. H. Arnold as observing that "[d]estruction is too cheap, too easy").

[50] The earliest use of this phrase as a reference to the horrors of World War II may have been in the documentary film "Mein Kampf," originally "Den Blodiga Tiden," by German filmmaker Erwin Leiser. THE YALE BOOK OF QUOTATIONS 451 (Fred. R. Shapiro, ed., 2006).

[51] Francis Biddle, *The Nurnberg Trial*, 33 VA. L. REV. 679 (1947).

[52] Geneva Convention (I) for the Amelioration of the Condition of Wounded and Sick in Armed Forces in the Field, Aug. 12 1949, 75 U.N.T.S. 31 [hereinafter G.C. (I)]; Geneva Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea of Aug. 12, 1949, 6 U.S.T. 3217 [hereinafter G.C. (II)]; Geneva Convention (III) Relative to the Treatment of Prisoners of War of Aug. 12, 1949, 6 U.S.T. 3316 [hereinafter G.C. (III)]; Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War of Aug. 12, 1949, 6 U.S.T. 3516 [hereinafter G.C. (IV)].

[53] The newest independent nation, South Sudan, ratified all four of the 1949 conventions on Jan. 25, 2013. *Treaties, States Parties and Commentaries: South Sudan*, INT'L COMM. OF THE RED CROSS (last visited May 22, 2016), https://www.icrc.org/applic/ihl/ihl.nsf/vwTreatiesByCountrySelected.xsp?xp_countrySelected=SS&nv=4.

[54] *See* G.C. (I), *supra* note 52, at art. 50; G.C. (II), *supra* note 52, at art. 51; G.C. (III), *supra* note 52, at art. 130; G.C. (IV), *supra* note 52, at art. 147.

[55] G.C. (I), *supra* note 52, at art. 49.

[56] Thus, both civilians and military officers stood trial at the International Military Tribunal at Nuremberg. TELFORD TAYLOR, THE ANATOMY OF THE NUREMBERG TRIALS 89-90 (1992).

term for any offense for which the identity of the perpetrator is irrelevant, and hence for which combatant immunity is not a defense, as all of the non-belligerency offenses chargeable in military commissions can be analogized to one or more of Geneva's grave breaches.[57]

Unfortunately, the nature of the two types of crimes, and the fact that they were often tried in the same military tribunals, have led to mistakes about the way liability is treated between them. Because courts and commentators have not always recognized the difference between the two species of crimes at issue, there is sometimes confusion as to whether or not the law of armed conflict permits or forbids conviction for conspiring to commit a crime.[58]

For a variety of reasons, not least among them ease of prosecution, the current commissions have focused on belligerency offenses.[59] Unfortunately, the United States has attempted to establish liability for inchoate offenses in trials by military commission. Courts have generally rebuffed these efforts, which have resulted in Asculum defeats for two successive administrations. Had the prosecution won more of these battles, the future would be a much bleaker place for American interests as well as the international order.

II. ALL OUR YESTERDAYS: A COLLECTION OF PROSECUTION VICTORIES AND DEFEATS

A. Seemingly Easy Wins

During the initial phase of the military commissions, their irrelevance appeared to be their most consistent feature.[60] After the

---

[57] G.C. (IV), *supra* note 52, at art. 147.

[58] *Compare* Al Bahlul v. United States, 792 F.3d 1, 10 (D.C. Cir. 2015) ("[t]he government concedes that conspiracy is not a violation of the international law of war.") *with id.* at 49 (Henderson, J. dissenting) ("the Congress has taken a preexisting international law-of-war offense—conspiracy to commit war crimes—and eliminated one element.").

[59] *See infra* Part II.

[60] Alexander, *supra* note 12, at 1119 ("Within two months of the executive order decreeing that suspected terrorists should be tried exclusively in military

initial presidential order of November 2001 announcing the use of military commissions,[61] scholars and commentators watched eagerly to see what procedures would develop and who would be subject to them.[62] The first set of potential procedures, issued in March 2002,[63] were met with a barrage of commentary, much of it critical.[64] Over time, both internal and external challenges to the commissions caused the rules to be issued, amended, reissued,[65] and ultimately made the subject of formal legislation.[66] By the time Congress stepped into the fray in December 2006, there had still not been a single trial on the merits during the more than five years of the military commission effort. Likely feeling uneasy about having

commissions, three high-profile criminal prosecutions of alleged al Qaeda or Taliban members were brought in federal court.").

[61] Detention, Treatment, and Trial of Certain Non-Citizens in the War against Terrorism, 66 Fed. Reg. 57833 (Nov. 13, 2001).

[62] *See, e.g.*, Michael J. Kelly, *Understanding September 11-An International Legal Perspective on the War in Afghanistan*, 35 CREIGHTON L. REV. 283, 283-93 (2002); Neal K. Katyal & Laurence H. Tribe, *Waging War, Deciding Guilt: Trying the Military Tribunals*, 111 YALE L.J. 1259, 1259-1310 (2002); Harold Hongju Koh, *The Spirit of the Laws*, 43 HARV. INT'L L. J. 23, 23-40 (2002); Ronald C. Smith, *The First Thing We Do, Let's Kill All the Terrorists*, 16 CRIM. JUST. 1, 1 (2002); Charles V. Pena, *Blowback: The Unintended Consequences of Military Tribunals*, 16 NOTRE DAME J. L. ETHICS & PUB. POL'Y 119, 119-32 (2002).

[63] Dep't of Def., Military Comm'n Order No. 1, Procedures for Trials by Military Commissions of Certain Non-United States Citizens in the War against Terrorism (21 Mar. 2002).

[64] *See, e.g.*, Gerard J. Clark, *Military Tribunals and the Separation of Powers*, 63 U. PITT. L. REV. 837, 837 (2002); Robert John Araujo, S.J., *A Judicial Response to Terrorism: the Status of Military Commissions under Domestic and International Law*, 11 TUL. J. INT'L & COMP. L. 117, 118 (2003); Kathleen M. McCarroll, *With Liberty and Justice for All: the November 13, 2001 Military Order Allowing the Use of Military Tribunals to Try Those Suspected of Aiding Terrorists Violates the Rights Guaranteed to Noncitizen United States Residents under the Constitution*, 80 U. DET. MERCY L. REV. 231, 232 (2003); Curtis A. Bradley and Jack L. Goldsmith, *Congressional Authorization And The War On Terrorism*, 118 HARV. L. REV. 2047, 2049 (2005); Srividhya Ragavan and Michael S. Mireles, Jr., *The Status of Detainees from the Iraq and Afghanistan Conflicts*, 2005 UTAH L. REV. 619, 619-76 (2005).

[65] David Glazier, *A Self-Inflicted Wound: A Half-Dozen Years of Turmoil Over the Guantánamo Military Commissions*, 12 LEWIS & CLARK L. REV. 131, 150-51 (2008) (recounting the issuance of various rules and orders over a two-year period).

[66] After the Supreme Court rejected the executive branch procedures in *Hamdan v. Rumsfeld*, Congress enacted the Military Commissions Act. *See* M.C.A., *supra* note 15; *see also infra* notes 111-14 and accompanying text.

created a system that did not seem to have any ability to function, the government was in sore need of an easy win.

1. The Easiest Case: The Story of David Hicks

The first conviction exemplified such a win. David Matthew Hicks,[67] born in Australia, had converted to Islam in 1999, traveled to Albania,[68] and later to Afghanistan, to study the Quran and train with Al Qaeda.[69] After courses in surveillance and urban warfare, he briefly went to Pakistan to visit a friend, where he saw televised coverage of Al Qaeda's attack on the United States.[70] Shortly after the September 11 attacks he sought to return to Afghanistan to join Al Qaeda there.[71] By mid-December he had been captured by the Northern Alliance while attempting to flee in a taxicab he had paid for by selling his weapon.[72]

Over the course of the next several years, the battles over the fate of David Hicks shifted from some of the most brutal military conflicts of the early 21st century to legally and politically charged conflicts on two continents.[73] In Australia, the government of Prime Minister John Howard had no interest in withdrawing Hicks from American custody, or preventing his trial by military commission.[74]

---

[67] *See* United States v. Hicks, No. 0002 (Office of Military Comm'ns, Guantanamo Bay, Cuba, March 26 & 30, 2007) [hereinafter Hicks ROT].
[68] *Id.* at 200.
[69] *Id.* at 102.
[70] *Id.* at 108.
[71] *Id.* at 109.
[72] *Id.* at 116.
[73] Or three; because his mother was a citizen of the United Kingdom, attorneys for David Hicks fought to have him awarded British citizenship. Although the courts ordered the government to grant him citizenship, British Home Secretary John Reid did so only to revoke it hours later, using his power to find that Hicks posed "a threat to the national security of the United Kingdom." Vikram Dodd, *Reid Revoked Citizenship of Guantánamo Detainee*, THE GUARDIAN (Jan. 11, 2007).
[74] LEX LASRY, THE UNITED STATES V. DAVID MATTHEW HICKS: FINAL REPORT OF THE INDEPENDENT OBSERVER FOR THE LAW COUNCIL OF AUSTRALIA, GUANTANAMO BAY, CUBA 15-16 (2007) (Austl.) (noting the government position that Hicks had committed no crime under Australian law, but desiring that he be tried nevertheless, and characterizing his return before a U.S. trial as causing his freedom on "a technicality or loophole").

In the United States, a variety of parties attempted, in the name of all the detainees, to end the possibility of trials by such commissions.[75]

By March 2007, at the very time that the defense was raising a series of pretrial motions in the military commission, David Hicks was apparently ready to give in.[76] He offered a pretrial agreement with the government, which the convening authority of the military commissions accepted.[77] Under the terms of the agreement, Hicks would plead guilty to a single specification of material support for terrorism[78] and, among other conditions, refrain from discussing matters with the press for at least one year.[79] In return, the convening authority would dismiss the other charges and limit his sentence to no more than seven years,[80] no more than nine months of which would be unsuspended.[81]

The military panel that heard the sentencing evidence and arguments returned with a sentence of seven years,[82] and the convening authority approved it, suspending all but the initial nine months.[83] Within six weeks, David Hicks flew back to Australia to serve his unsuspended sentence in a maximum-security facility.[84] By

[75] *See* Coalition of Clergy, Lawyers, and Professors v. Bush, 310 F.3d 1153, 1153 (9th Cir. 2002) (holding that this group of citizens did not have standing to challenge the detention at Guantanamo Bay).
[76] LASRY, *supra* note 74, at 27 (including a motion to disqualify the military judge. After the guilty plea, the Australian observer characterized the motions hearing as "a contrived affair," and said it was designed "for public and media consumption").
[77] Hicks ROT, *supra* note 67, at 124. In military commissions, as in courts-martial, a pre-trial agreement is between the accused and the convening authority. In return for pleading guilty to some or all of the charged offenses, the accused receives the benefit of having the convening authority approve no more of the adjudged sentence than that set forth in the sentence limitation portion of the agreement. *See id.*
[78] *Id.* at 126.
[79] *Id.* at 129.
[80] *Id.* at 145.
[81] *Id.* at 146. As seven years of confinement was the maximum punishment for the specification to which Hicks pled guilty, the suspension was the core of the agreement. *See id.* at 147.
[82] Hicks ROT, *supra* note 67, at 245.
[83] *Id.* at 247 (suspension mandated by the convening authority during a post-trial action, May 1, 2007).
[84] Barbara McMahon, *Guantánamo Detainee Flies Back to Jail in Australia*, THE GUARDIAN (May 21, 2007).

the end of 2007, he had been released.[85] His release ended the formal confinement of the first person convicted by a U.S. military commission since the post-World War II period.[86]

2. The Slightly Less Easy Case of Omar Khadr

Omar Khadr's commission trial, like that of David Hicks, ultimately featured a guilty plea.[87] Unlike the Hicks proceedings, Khadr's involved a more sympathetic accused.[88] Hicks was characterized as a bad actor, a dispirited youth who had dropped out of his own society seeking to assist known terrorists in the accomplishment of their military objectives.[89] Omar Khadr, on the other hand, was merely a child when he first became involved with the U.S. War on Terror.[90] Although he was a Canadian citizen, born in Toronto, Khadr's parents moved the family back and forth between Canada and their home country of Pakistan during the first few years of his life.[91] By 1996, then nine-year-old Khadr and his family had moved to Afghanistan.[92] They were there during the U.S. fight against the Taliban, and a conflict between a U.S. military reconnaissance party and Khadr's father and uncle led to Khadr's wounding and capture in 2002.[93]

---

[85] Barbara McMahon, *Australia Frees its Guantanamo Terror Inmate*, THE GUARDIAN (Dec. 28, 2007).

[86] William Colepaugh, an American citizen convicted by military tribunal at the end of the war, was paroled in 1960, PIERCE O'DONNELL, IN TIME OF WAR 285 (2005).

[87] United States v. Khadr, No. 0766, at 4673 (Office of Military Comm'ns, Guantanamo Bay, Cuba Aug. 9-12, 2007, Oct. 25-31, 2010) [hereinafter Khadr ROT].

[88] Frakt, *supra* note 35, at 752-53.

[89] Hicks ROT, *supra* note 67, at 204 (prosecution sentencing argument that Hicks "freely chose to walk away from those freedoms [election, religion, and association] to assist Al Qaeda).

[90] Khadr ROT, *supra* note 87, at 4838.

[91] United States v. Khadr, Stipulation of Fact, Prosecution Ex. 12, 13 (Oct. 2010) p. 3.

[92] *Id.* at 4 (noting that Khadr met "senior al Qaeda leaders" between the ages of 9 and 14).

[93] *See* United States v. Khadr, No. 13-005, at 7-8 (USMCR Stipulation of Fact, Guantanamo Bay, Cuba, Oct. 13, 2010). One interrogator at Bagram Air Base, who described himself as being known as "Monster," reported that Khadr's chest wound was "so large that one could fit a can of Copenhagen inside his chest," and that the

American forces took 16-year-old Khadr to Guantanamo Bay, where in a trial by military commission the prosecution noted that he had used weapons to attack and kill American soldiers,[94] even though he was not a member of a proper armed force.[95] Because he was a minor, much criticism focused on the United States' decision to treat him the same way that it treated adults. Most of the scholarly discussion of the Khadr case concerned this aspect of the prosecution. Many commentators found something unseemly, if not illegal, about the prosecution of a child soldier.[96] Less common, but perhaps more significant, was the critique that Khadr had been in a group of family members returning an attack by combatant forces.[97]

In October 2010, Khadr mimicked Hicks in pleading guilty in return for a limit on his sentence, which would be followed by a return to Canada.[98] The commission sentenced him to confinement for 40 years,[99] but the agreement limited the amount that the convening authority could approve to 8 years.[100] In September 2012,

interrogators called Khadr "Buckshot Bob" because his face "looked like he'd been blasted with a shotgun," Defendant's Exhibit K at 1, United States v. Khadr, No. 13-005 (USCMCR 2008).

[94] Khadr ROT, *supra* note 87, at 4830 (prosecution opened its closing argument by calling Khadr "a terrorist and a murderer").

[95] Frakt, *supra* note 35, at 752 (calling Khadr "the clearest example of a detainee being prosecuted and convicted for direct participation in hostilities.").

[96] *See, e.g.*, Christopher L. Dore, *What to do with Omar Khadr? Putting a Child Soldier on Trial: Questions of International Law, Juvenile Justice, and Moral Culpability*, 41 J. MARSHALL L. REV. 1281, 1320 (2008) ("Omar cannot shoulder the blame of his actions alone. At fifteen, he was a product of his environment, and lacked the resources, the moral motivation, and the developmental capabilities to escape the circumstances that placed him on a battlefield in the Afghan countryside.").

[97] Glazier, *supra* note 65, at 186 ("Khadr would have the legal status of a deer during hunting season – fair game for coalition forces to kill at will yet possessing no right to fight back.").

[98] Frakt, *supra* note 13, at 51 (crediting the work by Khadr's lawyers litigating and lobbying in Canada for the ultimate acceptance by the U.S. of the plea deal).

[99] Khadr ROT, *supra* note 87, at 4890.

[100] *See* United States v. Khadr, No. 13-005, at 6 (USMCR Offer for Pre-trial Agreement, Guantanamo Bay, Cuba, Oct. 13, 2010).

he returned to Canada.[101] A Canadian court ordered his release on bail in May 2015.[102]

In the cases of both David Hicks and Omar Khadr, the guilty pleas by defendants seeking to end what must have seemed like possibly perpetual pre-trial confinement avoided troubling legal issues. Military practice, like its civilian counterpart, includes a robust doctrine of waiver. A guilty plea makes most legal errors unreviewable by appellate courts.[103] Unfortunately for the stability of the military commissions' prosecution effort, some accused were to be convicted only after a full trial. That would allow them to continue to litigate the legal bases of their guilt, bases on which the guilt of David Hicks and Omar Khadr was also founded. Courts would eventually turn even these simple tactical victories into strategic defeats.[104] Unbeknownst to those prosecutors, however, these were Asculum defeats, temporary setbacks preventing far worse future outcomes.

B. Seemingly Tougher Losses

In light of their respective appellate proceedings, neither Hicks nor Khadr truly presented easy cases. At the time, however,

---

[101] *Omar Khadr Returns to Canada*, CBC NEWS (Sept. 29, 2012, 6:43 AM), http://www.cbc.ca/news/canada/omar-khadr-returns-to-canada-1.937754.

[102] The Canadian government appealed the decision, and lost in July, 2015. *Khadr's Release on Bail 'Disappointing,' Says Public Safety Minister,* CBC NEWS (May 7, 2015, 9:59 AM), http://www.cbc.ca/news/canada/edmonton/omar-khadr-s-release-on-bail-disappointing-says-public-safety-minister-1.3064945.

[103] DAVID A. SCHLUETER, MILITARY CRIMINAL JUSTICE: PRACTICE AND PROCEDURE § 14-3(B)(3) at 779 (8th ed. 2012) ("A plea of guilty will, as a general rule, waive all objections or issues that are not jurisdictional or deprive an accused of due process.").

[104] In 2015, the Court of Military Commission Review set aside the findings of guilt and sentence of David Hicks. Hicks v. United States, 94 F. Supp. 3d 1241, 1247-48 (C.M.C.R. 2015). The pretrial agreement had required Hicks to waive not only pretrial motions but also post-trial appellate review. Unfortunately for the United States, the Rule for Military Commissions provision at issue, 950c, required any such waiver to occur not less than ten days after the Convening Authority took action. Because Hicks's only waiver came during the trial, and thus before action, the Court set aside his waiver. *Id.* at 1243. Having done so, they quickly disposed of the case because of the intervening holding of the al Bahlul court that material support to terrorism in these commissions violated the ex post facto clause. *Id.* at 1247-48.

they seemed to be almost absurdly uncomplicated, as each involved a voluntary guilty plea by a citizen of an allied nation eager to return to his homeland. The other cases, some of which also involved guilty pleas, were significantly more complicated. Because the detainees in the next two prominent cases were convicted notwithstanding their pleas, they were able to litigate their legal objections to the military commissions. That litigation subsequently led to Asculum defeats for the prosecution.

1. *Hamdan*, the Supreme Court, and a Second Chance

The first of these, and the military commission case that has reached the highest level of judicial resolution, involved the former driver and bodyguard of Osama Bin Laden, Salim Hamdan.[105] After Hicks, Hamdan was the second accused to face trial by commission. Unlike Hicks, he pled not guilty, but was ultimately convicted of five specifications of material support for terrorism.[106] Before the conviction, however, he managed to change the face of American law.[107] While the initial set of charges, which were preferred under the rules established by the Department of Defense in 2002,[108] were pending, he sought the intervention of federal courts.[109] He argued that the military commissions had no jurisdiction over conspiracy under either U.S. statutory or international law, and that the procedures for the current commission violated both international and domestic law. Hamdan took his case as far as the U.S. Supreme Court,[110] where a majority agreed that congressional limitations and the Geneva Conventions of 1949 prevented his trial in the tribunal as it was then constituted.[111]

[105] Hamdan v. Rumsfeld, 548 U.S. 557 (2006).
[106] Hamdan v. United States, 696 F.3d 1238, 1244 (D.C. Cir. 2012).
[107] *Hamdan*, 548 U.S. at 678 (Thomas, J., dissenting) (arguing that the Court "openly flouts our well-established duty to respect the Executive's judgment in matters of military operations and foreign affairs").
[108] Hamdan v. Rumsfeld, 344 F. Supp. 2d 152, 154 (D.D.C. 2004).
[109] *Hamdan,* 548 U.S. at 567 (majority opinion).
[110] *Id.* at 557.
[111] *Id.* at 567. Four justices would also have held that conspiracy was not a crime under the international law of armed conflict. *Id.* at 610 (plurality opinion). Because the extant support for the military commissions was limited to those

Within six months of that decision, Congress responded by passing the Military Commissions Act ("MCA"),[112] which addressed the defects noted by the Court.[113] New charges were preferred under the new law,[114] and it was these that ultimately led to Hamdan's convictions.[115] Of great interest at the time was the perceived lenity of the sentence imposed by the commission: the decision to grant credit for time served before trial meant that Hamdan would be eligible for release before President Bush even left office.[116] And although there remained the possibility that the United States would continue to detain Hamdan as a combatant after he served his punishment, the United States ultimately transferred Hamdan to Yemen in November 2008.[117]

After his release, however, Hamdan did not stop fighting. He continued to seek post-conviction relief,[118] arguing that even the new charges were unsound as a matter of domestic and international

---

offenses triable by statute or by the law of war, and no statute then authorized trials by military commissions for conspiracy, these justices would have held conspiracy to be beyond the reach of military commissions. Two other justices joined Justice Thomas' dissent on this point. *Id.* at 697-98. Justice Kennedy would not have decided this question. *Id.* at 655 (noting that "Congress may choose to provide further guidance in this area"). Chief Justice Roberts, having been a member of the Court of Appeals for the D.C. Circuit that decided the case below, did not participate.

[112] 10 U.S.C. §§ 948a-950w (2006).

[113] Responding, perhaps, to Justice Kennedy, the Military Commissions Act provided for the trial of conspiracy as a criminal offense. 10 U.S.C. § 950 t(29).

[114] Hamdan v. United States, 696 F.3d 1238, 1243-44 (D.C. Cir. 2012).

[115] *Id.* at 1240-41 (stating that he was sentenced to sixty-six months of confinement, with credit for time served).

[116] Military Judge Ruling on Motion for Reconsideration and Re-Sentencing, P-009 (Oct. 29, 2008). It seems to have been the decision to grant pretrial confinement credit that most troubled the government, who appealed this point and lost. *Id.*

[117] Robert F. Worth, *Bin Laden Driver to Be Sent to Yemen*, N.Y. TIMES (Nov. 25, 2008). According to Prof. Charles Schmitz, an expert in Yemen who assisted his legal team, reports that Hamdan is still living in Yemen as of the time of this writing, "struggling like the rest of Yemen to make ends meet during the war." E-mail from Charles Schmitz, Professor, Towson University, to author (Aug. 19, 2015) (on file with the author).

[118] *Hamdan*, 696 F.3d at 1241.

law.[119] Using the appellate right granted by the MCA,[120] he asked the D.C. Circuit Court to overturn of his conviction.[121] That Court agreed with him that the offenses with which he had been charged did not, in fact, violate the law governing armed conflict.[122]

The D.C. Circuit Court, in Hamdan's second trip through the federal courts ("Hamdan II"), concluded that Congress had not intended to authorize punishment by military commissions for acts that preceded the enactment of the MCA, if those acts were not already criminalized under the international law of war.[123] Determining that material support for terrorism was in fact a new offense, the Court reversed Hamdan's conviction and sentence.[124] As a legal matter, the most celebrated military commission victory quietly became another defeat for the government.

2. The Many Cases of al Bahlul

Ironically, Hamdan's victory may ultimately be limited to him personally. The most recent round of battles involved Ali Hamza Ahmad Suliman al Bahlul.[125] Like Hamdan, he had been close personally to Osama bin Laden. Unlike Hamdan, who was primarily a driver,[126] Bahlul was a more senior official in Al Qaeda, serving as a media producer for the organization.[127] After the destroyer USS *Cole* was attacked in 2000, Bahlul prepared a video based on the attack for recruiting other potential jihadists for Al

[119] *Id.* at 1244 (explaining that the military commissions had acquitted Hamdan of the sole specification of conspiracy, but convicted him of five specifications of the charge of material support for terrorism).
[120] 10 U.S.C. § 950g (2012). The statute grants to that court "exclusive jurisdiction to determine the validity of a final judgment rendered by a military commission (as approved by the convening authority and, where applicable, as affirmed or set aside as incorrect in law by the United States Court of Military Commission Review)." *Id.*
[121] *Hamdan*, 696 F.3d at 1241.
[122] *Id.*
[123] *Id.* at 1247 (stating that "[c]ongress believed that the Act codified no new crimes and thus posed no ex post facto problem").
[124] *Id.* at 1250 (explaining that "the issue here is whether material support for terrorism is an international-law war crime. The answer is no.").
[125] See Al Bahlul v. United States, 792 F.3d 1, 3 (D.C. Cir. 2015).
[126] *Hamdan*, 696 F.3d at 1242.
[127] Al Bahlul v. United States, 767 F.3d 1, 5 (D.C. Cir. 2014).

Qaeda.[128] Bin Laden was sufficiently impressed that Bahlul became the primary public relations officer for the organization, and he prepared the "martyrs' wills" for two of the September 11 hijackers, Mohammed Atta and Ziad al Jarrah.[129]

By December 2001, Pakistani officials had captured Bahlul and turned him over to the United States.[130] In 2004, the United States charged him in a military commission with conspiracy to commit war crimes,[131] but the trial was delayed pending the resolution of Hamdan's case through the federal court system.[132]

After the *Hamdan* decision in the Supreme Court, and subsequent passage of the MCA, the government preferred charges corresponding to some of the offenses in the statute: conspiracy and solicitation to commit war crimes, and the provision of material support to a terrorist organization.[133]

Significantly, the conspiracy and solicitation offenses included specifications that fit both categories of law of war violations. On the one hand, the charges included grave breaches such as murder of protected persons.[134] On the other hand, the charge sheet made reference to belligerent acts: Bahlul's conspiracy to commit "murder in violation of the law of war" and "destruction

[128] *Id.* at 5-6.
[129] *Id.* at 6.
[130] *Id.*
[131] In the first set of proceedings, under the presidential order, al Bahlul was charged only with conspiracy. *See* Review of Charge and Recommendation at 4-7, United States v. Al Bahlul (June 28, 2004). That charge, though, included specific references to grave breaches such as "attacking civilians" and "attacking civilian objects," as well as belligerency offenses such as "murder by an unprivileged belligerent" and "destruction of property by an unprivileged belligerent." *Id.* at 5-6.
[132] *Al Bahlul*, 767 F.3d at 6.
[133] *Id.* at 6-7.
[134] Appellate Ex. 059 at 1-2, United States v. Al Bahlul [hereinafter Flyer]. A "flyer" is the document provided by prosecutors to military panels in courts-martial and commission proceedings that provides the final form of the charges against the accused without the other information contained on the charge sheet. *See* Danielle Tarin, *Rules and Law Governing Flyers, Cleansed Charge Sheets, and Flimsies*, ARMY LAW., June 2013 at 25, 27.

of property in violation of the law of war."[135] Although the title of these offenses suggests that they may not be mere belligerency offenses, the text of the statute makes clear that they are.[136]

Bahlul pleaded not guilty, asserting that the military commission had no authority to try him.[137] He nonetheless freely admitted to the factual basis of the charges.[138] The commission, unsurprisingly, convicted him of all three charges and sentenced him to confinement for life.[139] For the government, the story of Bahlul seemed to have ended well. But the story had only begun.

Only Hamdan has had a more complex judicial journey than al Bahlul.[140] As noted, a panel of the D.C. Circuit had already decided in Hamdan II that material support for terrorism was not a crime under international law, and hence was not triable for events that occurred before the passage of the MCA.[141] Because Bahlul's conviction included two other offenses, this decision did not end his story as it had Hamdan's. A panel of the D.C. Circuit first determined that all three of the offenses fell because of the logic of the Hamdan II opinion, as the existence of none of the three predated the MCA.[142]

---

[135] Flyer, *supra* note 134, at 1.
[136] For example, the statute defines the former as "[a]ny person subject to this chapter who intentionally kills one or more persons, *including privileged belligerents*, in violation of the law of war . . ." 10 U.S.C. § 950t (15) (2009) (emphasis added). The only reason for the inclusion of the italicized language is to ensure that the military commissions will consider the attack on a legitimate target, when done by an unprivileged person, to be a crime.
[137] *Al Bahlul*, 767 F.3d at 7.
[138] *Id.* His trial was never a model of a professional justice system: he attempted to fire his lawyers and proceed pro se, but then absented himself from the proceedings on several occasions by refusing to leave his cell; he made neither opening statement nor closing argument, never objected to any prosecution evidence, and presented no defense. *Id.*
[139] *Id.* at 7-8.
[140] At the time of writing, al Bahlul's legal journey is not yet complete.
[141] *Al Bahlul*, 767 F.3d at 8.
[142] *Id.*

The full court then took up the case en banc.[143] It agreed that neither solicitation[144] nor material support were a part of the international law of armed conflict, although it expressly purported to overturn Hamdan II in doing so.[145] The Court found that Congress had, in fact, expressly intended to criminalize conduct that occurred before passage of the MCA, but in doing so had violated the Ex Post Facto Clause. It found that by importing material support for terrorism and solicitation into the jurisdiction of the military commissions, Congress had violated that clause of the Constitution because these offenses had historically not been "triable by military commissions" under the law of armed conflict. Hence, those two offenses only became triable upon the enactment of the MCA. It was thus plain error to convict Bahlul of offenses that only became offenses when Congress acted in 2006, five years after the United States took him into custody.[146]

The full court disagreed about conspiracy, however, finding that the conspiracy charge avoided an Ex Post Facto problem because other U.S. criminal laws already prohibited the conduct at issue.[147] It also concluded that conspiracy was triable as an offense under the law of war, or at least that it was not plain error that it was not triable.[148] This result thus disposed of two of the charges against Bahlul, but in upholding the other, it did so against only one challenge, the argument that its promulgation in the MCA was an Ex Post Facto violation. The *en banc* court then remanded the case to

---

[143] *Id.*
[144] *Al Bahlul*, 767 F.3d at 30.
[145] *Id.* at 29.
[146] *Id.* at 31.
[147] *Id.* at 18 (citing 18 U.S.C. §2332b (2015); the court noted that military commissions cannot try violations of this statute, but held that the *Ex Post Facto* Clause does not limit procedural changes like forum).
[148] *Id.* at 10 (The court used the "plain error" standard because it found al Bahlul to have waived any objection based on the *Ex Post Facto* Clause. Although he objected to the characterization of his acts as crimes, the Court of Appeals found that this was not a question of law but "because they were inspired by religious fervor." This was despite the fact that the pro se litigant had objected to "the meaningless American laws" as an attempt to rewrite divine laws.).

the original panel to consider Bahlul's other challenges against the surviving conspiracy charge.[149]

The other shoe dropped for the government during that remand. A divided panel held that conspiracy was also a flawed charge.[150] The majority held that there was insufficient historical practice supporting the trial of offenses such as conspiracy before military commissions.[151] Lacking evidence of such practice, Congress was not free to assign the judicial power of this trial to a purely executive organization such as a military commission.[152] The court struck down the sole remaining charge, and with that, Bahlul's conviction by military commission went the way of those of David Hicks and Salim Hamdan.

III. THE ENEMY WITHIN: WHY THE PROSECUTION KEEPS LOSING

A somewhat surprising theme running throughout these cases is that many of these defeats have been handed to the military commission prosecutors by federal appellate judges.[153] Perhaps emboldened by the Supreme Court's pronouncements in *Hamdan*[154]

---

[149] *Al Bahlul*, 767 F.3d at 31 (he argued that Congress had exceeded its authority by defining crimes that were not recognized by the law of armed conflict, that the MCA violated Article III of the Constitution by allowing these same offenses to be tried, that his conviction violated the First Amendment, and that subjecting only aliens to the jurisdiction of the military commissions violated the Equal Protection clause.).
[150] Al-Bahlul v. United States, 792 F.3d 1, 37 (D.C. Cir. 2015).
[151] *Id.* at 36.
[152] *Id.* (Because such an assignment of judicial power to the executive branch violated the structural requirements of Article III, the court concluded, it was not subject to waiver, which had led the en banc court to reject the challenge to the conspiracy charge. Here the court applied a de novo review, which caused one of the judges who joined the opinion rejecting the Ex Post Facto challenge in 2014 to also join the opinion vacating the conspiracy conviction in 2015. (Tatel, J., concurring)).
[153] But federal appellate judges have not handed all of the defeats out. Earlier in the proceedings it was *military* judges who were finding that the procedures did not comport with the law. *See* United States v. Khadr, CMCR 07-001 (2007) (reversing decision by the military commission judge dismissing all charges s*ua sponte* based on lack of personal jurisdiction, because the Combatant Status Review Tribunal had only found Khadr to be an alien enemy combatant, but not an alien unlawful enemy combatant).
[154] *See generally* Hamdan v. Rumsfeld, 548 U.S. 557 (2006).

and *Boumedienne*,[155] a series of panels have been fairly consistent in rejecting the government's view of the law of armed conflict.[156] This is unusual, both because courts tend to be more deferential to the executive in areas of military and international operations,[157] and because a large number of well-respected commentators and scholars have advanced the government's position.[158] These defeats clustered around what seem to be two separate legal arguments, one over material support to terrorist organizations and the other over conspiracy as an offense in international law. These two strands are actually part of the divide between belligerency offenses and grave breaches, and that the unwillingness of the courts to countenance the stubbornly advanced government view in this area provided a series of defeats that ultimately rebounded to the benefit of the United States.

---

[155] Boumediene v. Bush, 553 U.S. 723 (2008) (recognizing a right of habeas corpus for detainees and holding that the Military Commissions Act was an unconstitutional suspension of that right).

[156] Frakt, *supra* note 35, at 762.

[157] *See, e.g.*, Munaf v. Geren, 553 U.S. 674, 700 (2008) ("it is for the political branches, not the Judiciary, to assess practices in foreign countries and to determine national policy in light of those assessments); Orloff v. Willoughby, 345 U.S. 83, 94 (1953) ("Orderly government requires that the judiciary be as scrupulous not to interfere with legitimate Army matters as the Army must be scrupulous not to intervene in judicial matters").

[158] The latest round of litigation in the case of al Bahlul saw the filing of amici briefs supporting the government by, inter alia, Professors Peter Margulies, Geoff Corn, Chris Jenks, and Eric Talbot Jensen, as well as former military judge advocates from the Army, Navy, and Air Force: retired Major Generals John D. Altenburg, Michael J. Marchand, Michael J. Nardotti, Jr., Rear Admiral Steven B. Kantrowitz, and Brigadier General Thomas L. Hemingway. Brief of Amici Curiae Former Government Officials, Former Military Lawyers, and Scholars of National Security Law in Support of Respondent as Amici Curiae Supporting Respondents, Al Bahlul v. United States, 412 U.S. App. D.C. 372 (No. 11-1324); Brief of John D. Altenburg, Maj. Gen., U.S. Army (Ret.), Steven B. Kantrowitz, Rear Adm., JAGC, U.S. Navy (Ret.), Michael J. Marchand, Maj. Gen., U.S. Army (Ret.), Michael J. Nardotti, Jr., Maj. Gen., U.S. Army (Ret.), Thomas L. Hemingway, Brig. Gen., U.S. Air Force (Ret.), Washington Legal Foundation, and Allied Educational Foundation as Amici Curiae in Support of Respondent, Supporting Affirmance as Amici Curiae Supporting Respondents, Al Bahlul v. United States, 412 U.S. App. D.C. 372 (No. 11-1324).

A. The Rejection of Material Support

As hinted at in the handful of cases that travelled the pipeline through the military commissions, the battle over whether a charge of material support is triable by such a commission was a significant reason that the effort proceeded at such a glacial pace. This offense, codified in 18 U.S.C. 2339A,[159] allows prosecutors to incapacitate participants in potential terrorist schemes of foreign organizations.[160] Although it has a solid foundation in the American criminal law context,[161] its inclusion in the initial list of punishable offenses published by the Secretary of Defense was odd. Certainly military commissions had never used a charge like material support for terrorism before. The inclusion of a wholly new crime, one based so completely on U.S. domestic law, seemed to violate the notion that military commissions existed to try offenses against the law of armed conflict.[162] Many commentators were puzzled, or even outraged, and the legal community never suggested that it welcomed this development.[163]

---

[159] 18 U.S.C. 2339A (2009). The parallel offense was made punishable by the Military Commissions Act, 10 U.S.C. §950t (25) (2009). The companion civilian offenses, including the frequently used Providing Material Support or Resources to Designated Foreign Terrorist Organizations, were not included in the MCA. 18 U.S.C. § 2339B (2015).

[160] *See* Robert M. Chesney, *The Sleeper Scenario: Terrorism-Support Laws and the Demands of Prevention*, 42 HARV. J. ON LEGIS. 1, 13-15 (2005) (discussing the passage of the initial version of the law after the first attack on the World Trade Center, and its expansion to criminalize more activities by supporters of terrorist organizations).

[161] *See, e.g.*, Holder v. Humanitarian Law Project, 561 U.S. 1, 7 (2010) (upholding the companion §2339B against a challenge based on the First Amendment).

[162] Margulies, *supra* note 13, at 67-68 (rejecting the view advanced by the government in the al Bahlul appeals that a separate "domestic" law of armed conflict allowed the U.S. to import into military commissions domestic offenses not recognized in the international law of armed conflict).

[163] *See, e.g.*, Jack M. Beard, *The Geneva Boomerang: The Military Commissions Act of 2006 and U.S. Counterterror Operations*, 101 AM. J. INT'L L. 56, 56-57 (2007); David J. R. Frakt, *Applying International Fair Trial Standards to the Military Commissions of Guantanamo*, 37 S. ILL. U. L.J. 551, 596-97 (2013); Jonathan Hafetz, *Policing the Line: International Law, Article III, and the Constitutional Limits of Military Jurisdiction*, 2014 WIS. L. REV. 681 (2014); David Weissbrodt and Andrea W. Templeton, *Fair Trials? The Manual for Military Commissions in Light of Common Article 3 and Other International Law*, 26 LAW & INEQ. 353, 400 (2008).

Material support as a charge was novel, but it was also easy to understand, and perhaps even easier to plead to.[164] Perhaps because it required no specific malevolent act by the accused,[165] it was the charge selected by Hicks and Khadr as the basis for the guilty pleas that would ultimately return them to their home countries.[166] The military commissions, like the courts-martial system, require the judge to inquire into the providence, the voluntariness and factual basis, of a guilty plea.[167]

Additionally, because the key players drafting the rules for the military commissions were military lawyers, they transferred to the military commissions the court-martial practice of allowing[168] the accused to agree with the prosecution on a confessional stipulation of fact.[169] The stipulation and the providence inquiry by the judge

---

Even active military officers were less than supportive of the decision to include this offense. *See* Maj. Dana M. Hollywood, *Redemption Deferred: Military Commissions in the War on Terror and the Charge of Providing Material Support for Terrorism,* 36 HASTINGS INT'L & COMP. L. REV. 1, 3 (2013).

[164] For an offense before a law of war tribunal, the elements for this offense are as anodyne as can be. Although one variant on the offense of providing material support for terrorism requires that the accused knew or intended that the provided resources would be used for carrying out an act of terrorism, the other requires the government to show only that the accused knew that the organization to which he provided resources had engaged in terrorism at some time. MANUAL FOR MILITARY COMMISSIONS, pt. IV ¶ 20 (2012) [hereinafter MMC].

[165] Holder v. Humanitarian Law Project, 561 U.S. 1, 16-17 (2010).

[166] *See Omar Khadr Returns to Canada*, CBC NEWS (Sept. 29, 2012, 6:43 AM), http://www.cbc.ca/news/canada/omar-khadr-returns-to-canada-1.937754; Barbara McMahon, *Guantanamo Detainee Flies Back to Jail in Australia*, THE GUARDIAN (May 21, 2007, 6:57 PM), http://www.theguardian.com/world/2007/may/21/australia.guantanamo.

[167] Although the very extensive inquiry into a court-martial guilty plea before the judge will accept it mandated by United States v. Care, 40 C.M.R. 247 (C.M.A. 1969), it is labeled "impracticable" by the governing regulation. *See* MMC, *supra* note 164, at pt. II, 910(e). Compare the requirements set forth by that rule with the corresponding rule for courts-martial, MANUAL FOR COURTS-MARTIAL, UNITED STATES, R.C.M. 910 (2012) [hereinafter MCM], and its implementation in the fifteen-page script for courts-martial, U.S. Dep't of Army, Pam. 27-9, MILITARY JUDGES' BENCHBOOK ¶¶ 2-2-1 to 2-2-8 (10 Sep. 2014) [hereinafter DA Pam. 27-9].

[168] In practice, "allowing" could be read as "requiring," as agreement to submit such a stipulation is generally a non-negotiable position of the United States in the pretrial negotiations. *See, e.g.*, Hicks ROT, *supra* note 67, at 124-26.

[169] MCM, *supra* note 167, pt. II, 705(b)(1).

might have been very difficult for an accused if he was asked to confess that he had committed genocide or some other grave breach of international law. It was undoubtedly much easier to admit, as Hicks did, that he "guarded a Taliban tank" and that "every day received food, drink, and updates on what was happening from the fat Al Qaeda leader in charge who was on a bicycle."[170] Khadr found it possible to admit that he was not a member of a militia or other armed force, that he trained to support Al Qaeda, that he planted Improvised Explosive Devices, and that he participated in a firefight in which he killed an American soldier and was himself wounded.[171] Such stipulations and pleas could later be explained in polite society, and would not necessarily brand the confessant as a bad person, in contrast to someone who signed a stipulation confessing to a grave breach of international humanitarian law.

The appellate process changed the nature of all of that precedent. Hamdan's conviction was solely for material support. Thus, his appellate challenge concerned only the legitimacy of material support for terrorism as a charge in military commissions. Because the D.C. Circuit held that it was not, the foundation stone for this entire run of prosecutions was jeopardized.[172] That decision was overturned by the *en banc* D.C. Circuit, but only by substituting an even more firm prohibition on the use of material support charges in military commissions.[173] As the battle shifted to an argument over conspiracy, the United States may have allowed the exclusion of material support from military commissions.[174]

---

[170] Stipulation of Fact at 5, United States v. Hicks (Mar. 29, 2007). Hicks also admitted to receiving training and spending two hours on the frontline near Konduz, Afghanistan, before it collapsed in the face of an armored assault by the Northern Alliance. Nothing in the stipulation even hints at responsibility by Hicks for any acts that this article would label grave breaches. *Id.*

[171] United States v. Khadr, Stipulation of Fact, Prosecution Ex. 12, 13 (Oct. 2010) p. 1, 5, 8.

[172] Hamdan v. United States, 696 F.3d 1238, 1241 (D.C. Cir. 2012).

[173] Al Bahlul v. United States, 767 F.3d 1, 29 (D.C. Cir. 2014).

[174] *See, e.g.*, Hicks, CMCR 13-004 at 2 (the government's position in the most recent Hicks litigation that if it lost the argument that Hicks had waived his right to appellate review, the Court of Military Commission Review "should decline to affirm the findings and sentence.") *But c.f.* Corn and Jenks, *supra* note 13, at 41-42

B. The Government's Odd Choice Regarding Conspiracy

1. The Recent Confusion about Conspiracy

When Hamdan challenged his ongoing military commissions,[175] the nature of his liability for the crimes charged was among the objections he raised.[176] When his case reached the Supreme Court,[177] the opinion's conclusion that the system procedurally violated the military commission statutes that Congress had long before passed[178] meant that the Court did not need to resolve the inchoate crimes issue.[179] Nonetheless, a four justice plurality (of eight, as Chief Justice Roberts had sat on the D.C. Circuit panel that had heard the case below)[180] would have held that conspiracy was not a crime under the law of armed conflict—and conspiracy was a much more defensible charge than material support.[181] The *Hamdan* opinion did not ultimately address the availability of material support, but because the opinion necessitated Congressional action, it did not matter. Congress acted that fall, and by December 2006, President Bush was able to sign the MCA.[182] This act not only resolved the objections of the *Hamdan* majority, it also attempted to insulate both detention and military commissions from future judicial review through habeas corpus,[183] and specifically

(acknowledging the limitations imposed upon material support charges in these cases by the Ex Post Facto clause but arguing that "when Congress legislates prospectively in this exigent area, deference and historic practice should usually trump the Article III concerns").

[175] Hamdan v. Rumsfeld, 344 F. Supp. 2d 152, 156 (D.D.C. 2004).

[176] *Id.*

[177] Hamdan v. Rumsfeld, 548 U.S. 557 (2006).

[178] References to military commissions had been made in Article 15 of the 1920 Articles of War, and were carried forward into its successor, the 1951 Uniform Code of Military Justice. *See* 10 U.S.C. § 821 (2006).

[179] *Hamdan*, 548 U.S. at 613.

[180] Hamdan v. Rumsfeld, 415 F.3d 33 (D.C. Cir. 2005).

[181] *Hamdan,* 548 U.S. at 610.

[182] M.C.A., *supra* note 15.

[183] Curtis A. Bradley, *The Military Commissions Act, Habeas Corpus, and the Geneva Conventions*, 101 AM. J. INT'L L. 322, 330 (2007). This was the provision struck down in Boumediene v. Bush, 553 U.S. 723 (2008).

included both conspiracy[184] and material support for terrorist organizations[185] as punishable offenses.

While the rejection by federal judges of material support for terrorism as an appropriate feature of law of war military commissions has been swift and consistent, conspiracy has been more complicated. Two historical examples have exacerbated the confusion: the Lincoln and Nuremberg trials. At each of these tribunals, conspiracy was a featured offense, and each was, at least arguably, a law of war military commission.

The Lincoln trials were built entirely on the charge of conspiracy.[186] Despite criticism for other reasons, they remain a precedent of outsized influence. Notably, in the dispute over the nature of conspiracy, judges of the D.C. Circuit sparred over their meaning. In the Bahlul case's 2014 trek to *en banc* review,[187] Judge Henderson, for the Court, observed that the Lincoln conspirator trial occurred well before the passage of the statute that allowed military commissions to try cases arising under the law of war.[188] This demonstrated that Congress "was no doubt familiar with at least one high-profile example of a conspiracy charge tried by a military commission."[189] Thus the Court concluded that convicting Bahlul of conspiracy did not violate the Ex Post Facto Clause.[190] Judge Kavanaugh agreed: just as Dr. Samuel Mudd[191] could be convicted of

[184] 10 U.S.C. § 950t (29) (2006).
[185] 10 U.S.C. § 950t (25) (2006).
[186] Al Bahlul v. United States, 767 F.3d 1, 24 (D.C. Cir. 2014).
[187] A panel of the circuit having vacated the convictions by the military commission based on the circuit's holding in Hamdan's 2012 case that such convictions violated the Ex Post Facto clause. *Al Bahlul*, 767 F.3d at 8.
[188] 10 U.S.C. § 821 (2006).
[189] *Al Bahlul*, 767 F.3d at 25.
[190] *Id.* at 18. Because the Court found that he had forfeited this challenge to the commissions, it only applied a plain error standard in concluding that it was not plain that conspiracy was not triable by a law of war military commission. *Id.*
[191] *See* Mudd v. Caldera, 134 F. Supp. 2d 138 (D.D.C. 2001) (a challenge by Dr. Mudd's descendants seeking a correction of the military record that would require the Secretary of the Army to clear the doctor's record of conviction. The Court found that Dr. Mudd was triable as one who was an accessory after the fact by aiding and abetting John Wilkes Booth); aff'd on other grounds, Mudd v. White, 309 F.3d 819 (D.C. Cir. 2002).

conspiracy to commit a war crime, so too could Bahlul.[192] Dissenting on this point, Judge Rogers responded that the Lincoln trials added nothing to the government's position; the conspirators were not charged with *inchoate* conspiracy, as the single charge noted that they had not only conspired but also completed the "offense of maliciously, unlawfully, and traitorously murdering the said Abraham Lincoln."[193]

The following year, the panel weighing Bahlul's separation of power challenge against the surviving conspiracy charge again found need to consult the Lincoln precedent.[194] This time, the Court split over the question whether that tribunal was properly considered a pure law of war commission, or one that also had a martial law source of jurisdiction, which would allow it to consider purely domestic crimes, such as conspiracy. With a century and a half of hindsight, the court might also have noted that there is arguably a limited amount of precedential value that should be drawn from a hastily convened trial designed to ensure the conviction of those believed responsible for the loss of the beloved leader who had just suppressed an insurrection threatening the very existence of the nation. As Justice Jackson noted in a similarly tense time, albeit in a wildly different context, military actions do not always "conform to conventional tests of constitutionality."[195]

2. The Lincoln Trial's Use of Conspiracy

Judge Rogers is correct that the trial of the Lincoln conspirators can only be fairly read to allow conspiracy as a form of liability for an offense that is completed.[196] What is more, the

[192] *Al Bahlul*, 767 F.3d at 69 (Kavanaugh, J., concurring in part and dissenting in part) ("The Lincoln conspirators were expressly charged with and convicted of *conspiracy*") (emphasis in original).
[193] *Id.* at 44 (Rogers, J., concurring in part and dissenting in part).
[194] *See supra* note 33 and accompanying text.
[195] Korematsu v. United States, 323 U.S. 214, 244 (1944) (Jackson, J., dissenting). At issue in that instance was the exclusion order during World War II that punished American citizens of Japanese descent that formed the basis of the conviction of Toyosaburo (Fred) Korematsu.
[196] *Ex parte* Mudd, 17 F. Cas. 954 (S.D. Fla. 1868) (rejecting Dr. Mudd's habeas petition after presuming guilt of the "charge on which they were convicted -- of a

conspiracy charged was not only of a completed offense, but an offense that would today be characterized as a grave breach. The killing of the president, in a civilian theater behind the lines of battle and after the surrender of virtually every major force in the field,[197] was a violation of the rules of war.[198] The Lincoln conspiracy hearings stand out for their unique nature, but do not establish a broader principle that inchoate conspiracy, especially as to belligerency offenses, is triable by military commissions. This is especially so in the absence of evidence of trials by military commission of any member of the Confederate government for recruiting, supporting, or deploying any of the irregular forces who were themselves potentially subject to trial.

3. The Limitations of Conspiracy at Nuremburg

The International Military Tribunal at Nuremberg for the Trial of Major War Criminals provides the clearest view of the reaction of the global community to the use of conspiracy for law of armed conflict violations. During the planning for the tribunal, the American lawyers included conspiracy as an offense.[199] The hope

conspiracy to commit the military crime *which one of their number did commit*") (emphasis added).

[197] HERMAN HATTAWAY & ARCHER JONES, HOW THE NORTH WON: A MILITARY HISTORY OF THE CIVIL WAR 676 (1983). Although Joseph Johnston's force vainly attempting to slow Sherman's trek through North Carolina did not surrender until two days after the assassination, the collapsing Confederate government had already ordered that they do so. *Id*.

[198] Attorney General Speed, in his opinion on the propriety of a military tribunal for the conspirators, does not suggest otherwise. Although it is true that he expounded at length on the nature of "secret participants in the hostilities," what this article has been characterizing as those who commit belligerency offenses, it was only to show that such persons were triable even when the civil courts were open. For the offense, he turned to Vattel, who he quoted for the proposition that assassination was "an offense against the laws of war, and a great crime." "Opinion on the Constitutional Power of the Military to Try and Execute the Assassins of the President," 11 Op. Att'y Gen. 297 (1865). Of course, as the title suggests, and Judge Henderson conceded, the Speed opinion was written after the fact, and might be read as rationalization of actions already taken. Al Bahlul v. United States, 767 F.3d 1, 25 (D.C. Cir. 2014).

[199] Elizabeth Borgwardt, *Re-Examining Nuremberg as a New Deal Institution: Politics, Culture and the Limits of Law in Generating Human Rights Norms*, 23 BERKELEY J. INT'L L. 401, 433 (2005).

and expectation was that the first group of trials could establish the liability, as conspirators, of both the major leaders of Germany and of several organizations. Subsequent trials of rank-and-file members could then follow, with the prosecution's responsibilities limited to showing membership by the accused in one of these organizations that had been pronounced a criminal conspiracy.[200]

As several onlookers attested, the inclusion of conspiracy caused consternation among the allies. The French in particular were disturbed by the possible extension of criminal liability through a doctrine that threatened to make small players in the system liable for the deeds of the great.[201] Nonetheless, the trial proceeded with conspiracy as an independent count alongside those for crimes against peace, war crimes, and crimes against humanity.[202]

When the verdict was read, it appeared that the judges had severely limited the role of conspiracy.[203] The judgment consolidated the first two counts, those of conspiracy and crimes against peace, and limited its consideration to "whether a concrete plan to wage war existed, and determin[ing] the participants in that concrete plan."[204] In so doing, they overtly rejected the argument by the prosecution that conspiracy extended liability to everyone who had participated significantly in the Nazi Party or German government. [205] Furthermore, although the prosecution argued that the concept of conspiracy extended to the other counts of the indictment, war

---

[200] *Id.*
[201] *Id.* at 437.
[202] *Indictment*, *in* I TRIAL OF THE MAJOR WAR CRIMINALS BEFORE THE INTERNATIONAL MILITARY TRIBUNAL, NUREMBERG, 14 NOVEMBER 1945 - 1 OCTOBER 1946, 27-68 (1947).
[203] A plurality of the U.S. Supreme Court characterized the tribunal's treatment of conspiracy by noting that it "pointedly refused" to recognize conspiracy to commit war crimes as a violation of the law of armed conflict, despite the prosecution asking it to do so. Hamdan v. Rumsfeld, 548 U.S. 557, 610 (2006).
[204] *Two Hundred and Seventeenth Day, Monday, 30 September 1946, Afternoon Session: The Law as to Common Plan or Conspiracy*, *in* XXII TRIAL OF THE MAJOR WAR CRIMINALS BEFORE THE INTERNATIONAL MILITARY TRIBUNAL, NUREMBERG, 14 NOVEMBER 1945 - 1 OCTOBER 1946, 467-68 (1947) [hereinafter *The Law as to Common Plan or Conspiracy*].
[205] *Id.* at 467.

crimes and crimes against humanity,[206] the tribunal rejected this notion as beyond the scope of the Charter.[207]

One way to distinguish the charge of waging aggressive war from the charges of war crimes, or crimes against humanity, is that small players can play no serious role in the waging of an aggressive war. To be a part of the "concrete plan" to initiate a war of aggression requires that one be a significant player in the governmental control of the nation. To kill or torture a prisoner, or to participate in genocide, requires no particular amount of power within the nation. By limiting conspiratorial liability in this way, the Nuremberg Tribunal prevented the creation of a regime in which mere membership in the National Socialist Party would establish criminal liability. Thus, the Nuremburg Tribunal approved of conspiracy as a violation of international law, but only in so restricted a form that the plan of massive subsequent trials simply did not occur.[208] After the trial, it became a commonplace understanding of international criminal law that conspiracy, as understood by the United States, had no role in international law.[209]

4. Conspiracy-Like Liability

Yet it is also true that some international trials have featured forms of criminal liability that look something like conspiracy. Both command responsibility and joint criminal enterprise bear some resemblance to the conspiracy, and both have solid footing in international law. Ultimately, however each requires that offenses be completed, is limited to use only in the area of grave breaches, and neither has ever played a role in a belligerency offense.

---

[206] Borgwardt, *supra* note 199, at 440.

[207] *The Law as to Common Plan or Conspiracy*, *supra* note 204, at 469.

[208] *The Prehistory of Corporations and Conspiracy in International Criminal Law: What Nuremberg Really Said*, 109 COLUM. L. REV. 1094, 1208 (2009) (noting that in the first major consideration of the issue in the subsequent proceedings to the Trial of the Major War Criminals, the court dismissed the conspiracy charges after argument by counsel but without a written opinion).

[209] *Id.* at 1100 (noting that the statute governing the International Criminal Court does not include conspiracy "largely at the insistence of lawyers from civil law countries, whose domestic traditions generally do not include criminal or civil liability for conspiracy").

a. Command Responsibility

Command responsibility is the requirement of the law of war that commanders bear actual liability for the wrongdoing of their subordinates.[210] The classic statement of such criminality is that commanders are responsible for the deeds of their subordinates if they order them before the fact or ratify them after.[211] This type of liability is common, and is seen not only in areas such as the international law of war, but even the rules of responsibility for attorneys in the United States.[212] Law of armed conflict command responsibility goes far, however, by also encompassing to those who know of wrongdoing by subordinates and fail to prevent it,[213] or, in one particularly strong version, those who merely should know of the wrongdoing, even if they do not.[214] Whichever version of command

---

[210] Danner & Martinez, *supra* note 36, at 120.

[211] So, for example, the International Criminal Court uses a standard of liability that makes criminally responsible any person who "Orders, solicits or induces the commission of such a crime which in fact occurs or is attempted." Rome Statute of the International Criminal Court art. 25(3)(b), July 17, 1998, 2187 U.N.T.S. 3 [hereinafter Rome Statute].

[212] MODEL RULES OF PROF'L CONDUCT r. 5.1(c) (AM. BAR ASS'N 2016) (declaring responsibility for a lawyer for the actions of another if the former lawyer "orders, or with knowledge of the specific conduct, ratifies the conduct involved").

[213] *See, e.g.*, Rome Statute, *supra* note 211, at art. 28

> (a) A military commander or person effectively acting as a military commander shall be criminally responsible for crimes within the jurisdiction of the Court committed by forces under his or her effective command and control, or effective authority and control as the case may be, as a result of his or her failure to exercise control properly over such forces, where:
>
> (i) That military commander or person either knew or, owing to the circumstances at the time, should have known that the forces were committing or about to commit such crimes; and
>
> (ii) That military commander or person failed to take all necessary and reasonable measures within his or her power to prevent or repress their commission or to submit the matter to the competent authorities for investigation and prosecution.

[214] The very strong version perhaps received affirmation in Yamashita. Many scholars have read the finding of guilt in that case to stand for the proposition that General Yamashita was legitimately punished for the sins of his troops even though he might not have known of them. *See, e.g.*, Major Bruce D. Landrum, *The Yamashita War Crimes Trial: Command Responsibility Then and Now,* 149 MIL. L. REV. 293, 297 (1995) (noting that some had described Yamashita as "a victim, an

responsibility one uses, however, it extends no liability to drivers, foot soldiers, or even propagandists for crimes committed by others. It thus offers no aid to the government in trials like those of Hamdan, Khadr, and Bahlul.

b. Joint Criminal Enterprise Liability

Joint Criminal Enterprise ("JCE"), on the other hand, does hold liable those who are not major players in their military force.[215] It resembles conspiracy in applying to all participants in the criminal activity.[216] It does that so thoroughly that the dissenting judge in the most recent decision in the Bahlul case argued that conspiracy *was* an international law of armed conflict offense, merely passing under the name JCE.[217] This is incorrect, however: while conspirators are, under the common law, liable for any offense committed by any member of the conspiracy at any time, provided only that the offense fits within the design of the conspiracy,[218] JCE is much narrower. It is never a stand-alone form of liability.[219] Additionally, even the most wide-ranging form of JCE announced by international

'honourable Japanese general' tried and executed on 'trumped-up charges,' the subject of a 'legalized lynching.'" (citations omitted)). On the other hand, it is difficult to say with certainty what Yamashita meant in the minds of those who decided the case: the panel functioned as a jury in that case, and issued an opinion that, as one scholar of the law of war noted, is subject to at least four interpretations, but none truly announced strict liability for commanders. Major William H. Parks, *Command Responsibility For War Crimes,* 62 MIL. L. REV. 1, 30-31 (1973).

[215] Danner & Martinez, *supra* note 36, at 104 (describing Tadic, the person on trial before the International Criminal Tribunal for the former Yugoslavia in whose case the doctrine was expounded, as "an enthusiastic but relatively low-level participant in the crimes that occurred in Bosnia in the early 1990s").

[216] *Id.* at 103.

[217] Al Bahlul v. United States, 792 F.3d 1, 48 (D.C. Cir. 2015) (Henderson, J., dissenting).

[218] Pinkerton v. United States, 328 U.S. 640, 647 (1946) (rejecting the argument that evidence of direct participation by a conspirator was necessary for that conspirator's conviction of a substantive offense committed by the conspiracy because "Each conspirator instigated the commission of the crime. The unlawful agreement contemplated precisely what was done. It was formed for the purpose. The act done was in execution of the enterprise.").

[219] Danner & Martinez, *supra* note 36, at 118.

tribunals limits liability of accused to those acts that are a "natural and foreseeable consequence" of the common purpose.[220]

It is true that the lack of formally outlined doctrinal limits might well allow future international tribunals to expand the net of this form of liability to match the remarkable scope of Anglo-American conspiracy law; it is also true that no international tribunal has done so.[221] Instead, the actual use of JCE has paralleled the way it was used by the Allies after World War II: in a series of cases trying persons for abuse of prisoners, there was clear evidence that a small group of defendants had committed a series of a bad acts, but no way to identify which individual committed which act.[222]

Although both command responsibility and JCE share features with conspiracy, they do so only with conspiracy as a form of liability for completed offenses. There is no precedent in the international law of armed conflict for conspiracy as a form of liability for an offense that is only in the planning stages. The successful domestic prosecutions of terrorists such as Ramzi Yousef, convicted and sentenced to life for a plot to destroy a passenger aircraft crossing the Pacific Ocean, would not have been possible in a military commission.[223] Furthermore, although the words used by

---

[220] *Id.* at 106 (quoting the Tadic case from the International Criminal Tribunal for the former Yugoslavia).

[221] *Id.* at 150 (noting that an expansion of JCE to hold liable a small player "for all the crimes visited upon Bosnian Muslims in the early 1990s would seem patently unjust" but that "no convictions representing such a gross extension of liability have yet been entered").

[222] *Id.* at 111. Professors Danner and Martinez, wary of a possible expansion of JCE, acknowledged that this sufficiently paralleled the Tadic case that announced JCE to justify that conviction, but warned that the language of the court was so broad that it might be misused to the detriment of the legitimacy of the international legal system. *Id.* at 167 (Liability theories that distort the contribution of individual defendants to the crimes that ultimately occurred run the risk, over time, of producing a record of a violent period that fails to capture how and why the crimes occurred").

[223] United States v. Yousef, 327 F.3d 56, 79 (2d Cir. 2003) (describing Yousef's conviction for conspiracy in a plot to destroy twelve U.S.-flagged aircraft with time bombs after they left Asia). This act of terror did not occur because Yousef and a co-conspirator inadvertently started a fire in their apartment, and responding authorities discovered both the laptop containing the plan and many of the chemicals needed to carry it out.

international tribunals would conceivably support an extension of liability to minor members for every crime committed by any member of their organization, those same international tribunals have consistently rejected the notion that the liability they were imposing paralleled conspiracy or membership in a criminal organization.[224]

5. The Limits of Conspiracy-Like Liability in Military Commissions

These two forms of liability apply only to grave breaches. This is powerfully illustrated by the use of the doctrine of command responsibility at Nuremberg and in the years since. It was utterly uncontroversial to hold leaders of the Nazi regime liable for offenses committed by those under their control.[225] Indeed, although some of the accused on trial after World War II argued that they were only subordinates, and that criminal liability did not apply to those who were "just following orders," the defense did not save its major proponents.[226] There does not seem to have been a defense of "just giving orders" proffered by the accused at the Trial of Major War Criminals or the subsequent proceedings. Command responsibility for grave breaches may have been one of the most consistently accepted features of the Nuremberg trials.

Yet there also does not seem to have been an attempt by the victorious Allies to punish any of those who ran the machinery responsible for recruiting, training, and deploying those individuals who were themselves convicted of belligerency offenses. Although several of the leaders of the Abwehr, the German intelligence service that operated the spy and saboteur programs, fell into Allied hands at the end of the war, they were not tried as the masters of prison camp

[224] Danner & Martinez, *supra* note 36, at 118.
[225] Adam Roberts, *Land Warfare: From Hague to Nuremberg, in* THE LAWS OF WAR: CONSTRAINTS ON WARFARE IN THE WESTERN WORLD 116, 135 (Michael Howard et. al. ed., 1994) (This notes that although conviction of individuals based on wartime acts was controversial in many ways, it was not so in regard to grave breaches involving the treatment of prisoners and civilians because it "cannot have been wrong to punish these clear violations of the most elementary principles of decency.").
[226] SOLIS, *supra* note 47, at 357.

guards and executioners had been.[227] The international community has simply never found conspiracy or either of the arguably conspiracy-like forms of liability to be appropriate in trials for crimes for which guilt is dependent on the identity of the accused as an unprivileged combatant.[228] Yet the U.S. military commissions in the war against Al Qaeda have focused on that exact circumstance. And it is exactly that circumstance that has been rejected time and again by appellate courts, both military and civilian.

IV. METAMORPHOSIS: WHEN LOSING IS WINNING

To characterize these prosecutorial setbacks as Asculum defeats requires recognizing them as strategic victories. That can only be true if they prepared the legal battlefield for future victories by the government, or at least helped it to avoid more serious defeats. It is possible that the consistent rejection of expanded liability for belligerency offenses has done both: in the case of the highest-profile detainee, Khalid Shaikh Muhammed ("KSM"), the self-professed mastermind of the September 11 attacks,[229] a reluctance to conduct a trial by military commission might prove a strategic victory for the government. Further, in the imaginable world of future conflicts, a recognition of conspiracy liability for belligerency offenses might well prove disastrous for U.S. interests.

---

[227] Indeed, General Erwin von Lahousen, who headed the organization, testified as a witness against former colleagues at Nuremberg. *See* PIERCE O'DONNELL, IN TIME OF WAR: HITLER'S TERRORIST ATTACK ON AMERICA 288 (2005).

[228] Of course, as every modern power has operated spy services and other clandestine agencies, there were any number of available targets for such prosecutions, had any nation so desired.

[229] Tung Yin, *Ending the War on Terrorism One Terrorist at a Time: A Noncriminal Detention Model for Holding and Releasing Guantanamo Bay Detainees*, 29 HARV. J. L. & PUB. POL'Y 149, 175 (2005) (noting that he developed the idea of hijacking airplanes to make them weapons, while Osama bin Laden had focused on blowing them up).

A. Tomorrow: The Puzzle of Khalid Shaikh Muhammed

1. A Military Commission Trial of KSM?

KSM came into U.S. custody in 2003, when the Pakistani Inter-Services Intelligence, possibly assisted by the U.S. Central Intelligence Agency, captured him.[230] In 2006, he was transferred to the Guantanamo Bay Naval Facility, and President Bush announced that he would face trial by military commission.[231] He was charged, and a motions battle began that would prevent any meaningful progress in this most important test of the military commissions system.[232] Because of the stops and starts that occurred in the much less weighty cases of people like Hamdan and Khadr, KSM's case had not even had a panel seated before the end of the Bush presidency.[233]

A trial by military commission of KSM is well within the historical use of such a commission. It would be a legitimate legal proceeding. The previous reconsidering of the functions of military commissions, however, suggests that it would not be a wise legal proceeding.

As noted earlier, there are three separate types of military commissions.[234] These three types, however, can be reorganized into two groups, based on their strategic function. Some of these commissions are necessary; others are merely useful. Both martial law and military government courts are necessary. Human society cannot long function at an advanced level without a means for determining liability when crimes occur. Martial law is a long-recognized temporary necessity in response to a breakdown in the

---

[230] Gregory S. McNeal, *A Cup of Coffee After the Waterboard: Seemingly Voluntary Post-Abuse Statements*, 59 DEPAUL L. REV. 943, 947 (2010).
[231] Dana Carver Boehm, *Guantanamo Bay and the Conflict of Ethical Lawyering*, 117 PA. ST. L. REV. 283, 292 (2012).
[232] Charges were not *preferred*, or formally initiated, until April 15, 2008, and referred to the military commission for trial by the convening authority on May 9, 2008. United States v. Khalid Shaikh Mohammed, Charge Sheet (May 2008).
[233] As of the date of publication, there has still been no panel seated, and no evidence offered. *See* Gordon Mehler & Philip Hilder, *It's High Time the 9/11 Five Were Brought to Trial*, NEWSWEEK (Sept. 8, 2015).
[234] *See supra* Section I.A.

civil government's ability to maintain ordered liberty.[235] Likewise, an occupation cannot be legitimate or successful if the occupier has no way to protect society from the predations of crime. In every area in which the military is the only authority, the military must take on this role, however ill-suited it may be to it.[236]

On the other hand, law of war commissions are never necessary.[237] Those accused of violating the law of armed conflict may be dealt with in many ways, from trial in ordinary domestic courts,[238] to military detention with release at (or after) the end of the hostilities,[239] to, in the view of some, summary execution.[240] When nations individually [241] or collectively [242] opt to establish such commissions, they do so due to their usefulness and not necessity.

---

[235] DINSTEIN, *supra* note 24, at 92 ("The framers of the Hague Regulations were afraid that the Occupying Power might tolerate pervasive turmoil and turbulence, not lifting a finger to prevent rampant anarchy from paralyzing the whole life of the civilian population.").

[236] *Ex parte* Milligan, 71 U.S. 2, 127 (1866) ("On the theatre of active military operations, where war really prevails, there is a necessity to furnish a substitute for the civil authority, thus overthrown, to preserve the safety of the army and society, and as no power is left but the military, it is allowed to govern by martial rule until the laws can have their free course.").

[237] Perhaps because there is always another option for such fora, they are not without limits. *See* Gerald Neuman, *Extraterritoriality and the Interest of the United States in Regulating Its Own,* 99 CORNELL L. REV. 1441, 1459 (2014) (noting that the *Boumediene* case rejected the extreme view suggested by *Verdugo-Urquidez* that foreign nationals involuntarily in U.S. territory have no constitutional protections).

[238] Alexander, *supra* note 11, at 1118 ("All of the acts that have been charged as military commission offenses are crimes under the U.S. Code and could be prosecuted as such.").

[239] Hamdi v. Rumsfeld, 542 U.S. 507, 518 (2004) ("The capture and detention of lawful combatants and the capture, detention, and trial of unlawful combatants, by 'universal agreement and practice,' are 'important incident[s] of war.") (quoting *Ex parte* Quinn, 317 U.S. 1, 30 (1942)).

[240] TAYLOR, *supra* note 56, at 29 (1992) (describing the original British desire at the close of World War II that the senior leaders of the Nazi regime be "punished by a joint decision of the Governments of the Allies").

[241] Diane F. Orentlicher, *Settling Accounts: The Duty to Prosecute Human Rights Violations of a Prior Regime*, 100 YALE L.J. 2537, 2560 n.91 (1991) (noting Israel's reliance on universal jurisdiction when prosecuting Adolf Eichmann for Nazi war crimes in a domestic court).

The primary purpose of law of war military commissions is education.[243] The existence of a trial, even in an unfamiliar military format, has showcased the offenses of the accused in an attempt to prevent others from imitating, or even admiring, the alleged wrongdoer.[244] That was arguably the primary accomplishment of the most-lauded set of military commissions, those that heard the cases of prominent Nazis at Nuremberg after World War II.[245] Some have argued that the same is true of the trial of the Nazi saboteurs during World War II, although there the purpose was at least in part the concealment of certain information.[246] It was reasonable for the United States to fear that the Third Reich would repeat its attempts with a more loyal group of saboteurs[247] had they known that the failure was largely due to a betrayal by one of the saboteurs upon his arrival by mini-submarine.[248] By conducting the trial in the closed setting of a secretive military commission, the Roosevelt administration was able to convey the incredible effectiveness of the Federal Bureau of Investigation to internal and external observers.[249]

---

[242] TAYLOR, *supra* note 56, at 25 (noting the initiation of the Inter-Allied Commission on the Punishment of War Crimes at the beginning of 1942).

[243] Regarding trying the Nazi leadership, Lt. Col. Bernays of the U.S. War Department wrote his wife that "[n]ot to try these beasts would be to miss the educational and therapeutic opportunity of our generation." Borgwardt, *supra* note 199, at 408-09.

[244] This is a role of tribunals in any situation in which a significant change of government leaves people seeking justice for past wrongs, an area referred to as transitional justice. Danner & Martinez, *supra* note 36, at 90 (citing the retrospective use of the term "transitional justice" regarding the Nuremberg trials).

[245] Rpt. from Robert H. Jackson, Sup. Ct. Justice, to Harry S. Truman, President of the U.S., *International Conference on Military Trials* (Oct. 7, 1946) (noting that the military commissions "…documented from German sources the Nazi aggressions, persecutions, and atrocities with such authenticity and in such detail that there can be no responsible denial of these crimes in the future…").

[246] O'DONNELL, *supra* note 86, at 121 ("What [Attorney General] Biddle did not tell the secretary of war, however, was that he did not want the press and public to know that both German teams had found it so easy to penetrate America's defenses.").

[247] *Id.* at 125.

[248] *See* LOUIS FISHER, MILITARY TRIBUNALS & PRESIDENTIAL POWER: AMERICAN REVOLUTION TO THE WAR ON TERROR 94 (2005).

[249] O'DONNELL, *supra* note 86, at 105. The German High Command named the attempt by the saboteurs of the Quirin case for Franz Pastorius, the poet who led the first German immigrant community in America, in 1683. *Id.* at 21. *See generally Ex parte* Quirin, 317 U.S. 1 (1942).

Although many have criticized the decision to try the saboteurs by military commission, Adolf Hitler made no significant further attempts to infiltrate the United States following the Quirin Group's failure.[250]

Bringing global attention to the cruelty of Al Qaeda, and the merciless way in which it chooses its victims, might go a long way toward reducing the ability of it and groups like it to recruit to their cause.[251] The pain of victims, splashed across the internet for all to see, is a powerful counter-recruiting tool. Indeed, one of the specific goals of the post-World War II trials was the ability to allow both sides to offer their best arguments for their behavior, counting on humanity to discern between them.[252] As Justice Robert Jackson noted in his closing argument, "[t]he future will never have to ask, with misgiving, what could the Nazis have said in their favor. History will know that whatever could be said, they were allowed to say."[253] Unfortunately, the convoluted legal proceedings of the current military commissions, and their use of trials for belligerency offenses, have undermined their ability to teach. While the Nuremberg trials were and continue to be viewed as role models for the expression of international outrage,[254] the U.S. War on Terror military commissions have caused massive criticism.[255] What might once have been a powerful forum for the denunciation of an evil breach of the gravest responsibilities of an interdependent world has

---

[250] O'DONNELL, *supra* note 86, at 284 (noting that the German Navy was reluctant to risk a U-Boat for another futile sabotage mission).

[251] Biddle, *supra* note 51, at 680 (quoting diplomat and author Harold Nicolson as noting that at the International Military Tribunal "the inhuman is being confronted with the humane, ruthlessness with equity, lawlessness with patient justice, and barbarism with civilization").

[252] As it is of other "transitional" trials, marking the ends of oppressive or evil regimes. *See* Allison Danner & Martinez, *supra* note 36, at 91.

[253] 19 TRIAL OF THE MAJOR WAR CRIMINALS BEFORE THE INTERNATIONAL MILITARY TRIBUNAL, NUREMBERG, 14 NOVEMBER 1945 – 1 OCTOBER 1946, at 399 (1948).

[254] TAYLOR, *supra* note 56, at 634-35 (1992); Theodor Meron, *Reflections on the Prosecution of War Crimes by International Tribunals*, 100 AM. J. INT'L L. 551, 552 (2006) ("The Nuremberg experiment in particular proved to be, as Justice Jackson had hoped, a triumph of reason.").

[255] Even by those who should logically be, or once were, supporters of the military commissions. Glazier, *supra* note 65, at 184 (2008) (describing the sudden departure from the commissions of Colonel Morris Davis).

now degenerated into an extraordinary court dismissed by many as a secretive cure for tortured confessions, and a means of imposing liability on hapless people who had the temerity to oppose the United States in its muscular overseas behavior. Lessons taught by a military commission in the case of KSM will simply not be learned.[256]

2. A Federal Trial of KSM?

One of the early announcements of President Obama's first Attorney General, Eric Holder, was that KSM would be transferred to New York City, where he would stand trial for the attacks in a federal court, not a military commission.[257]

This announcement led to outrage.[258] Within a year, a bipartisan group in Congress passed an appropriations bill that forbade the spending of federal dollars to transport any detained person from Guantanamo Bay to the United States, for trial or otherwise.[259] Although part of the rationale for this statute was the preservation of Guantanamo Bay as a detention center, part of the discussion focused on KSM himself.[260] Possibly with a sense of resignation, the Administration restarted military commission proceedings against KSM.[261]

The rejection of a federal trial for KSM was a disturbing development for two reasons. Due to the nature of the offenses KSM is accused of, his trial, similar to the trials of other high-profile

---

[256] Morris D. Davis, *Guantanamo's Charade of Justice*, N.Y.TIMES, Mar. 27, 2015, at A21 ("Guantanamo has come to symbolize torture and indefinite detention, and its court system has been discredited as an opaque and dysfunctional process."). Morris Davis is a retired Air Force Colonel who served as the third Chief Prosecutor of the Military Commissions.

[257] Alexander, *supra* note 11, at 572.

[258] Charles J. Dunlap, Jr., *Responses to the Ten Questions*, 37 WM. MITCHELL L. REV. 5150, 5166 (2011) (calling the opposition to a trial in the U.S. "a storm of political opposition").

[259] Alexander, *supra* note 11, at 588-89.

[260] 155 CONG. REC. H12993-01 (2009) (statement of Rep. Gohmert) ("He says, 'We ask to be near to God'-this Khalid Sheikh Mohammed, who our President is inviting to come to New York City. We fight you and destroy you and terrorize you.' Khalid Sheikh Mohammed said this in his pleading.").

[261] United States v. Khalid Shaikh Mohammed, Charge Sheet (May 2011).

detainees, would be qualitatively different from previous military commissions. KSM was accused of—and has announced responsibility for, on several occasions—the intentional targeting of non-combatants on a vast scale.[262] No one has the legal authority to do that. No combatant immunity exists that protects anyone from culpability if they commit a grave breach of the law of armed conflict. And there is no doubt that the hijacking of civilian aircraft to fly into civilian skyscrapers is a grave breach of international law.[263]

KSM's trial, therefore, would focus on what he did, not who he was. Unlike Hicks, Hamdan, Khadr, and the rest, KSM's charges relate to behavior that would be punishable by military commissions whether committed by civilians or military personnel.[264] It would, in that regard, resemble the trials of major war criminals in both Europe and the Pacific following World War II. There was no question that military officers like General Yamashita were proper combatants.[265] They could not have been punished for their efforts leading military operations against the Allies:[266] indeed, punishing proper combatants for their legitimate wartime activities is itself a

[262] *See, e.g.*, Verbatim Transcript of Combatant Status Review Tribunal for ISN 10024, at 18. *But cf.*, McNeal, *supra* note 230, at 951 ("The legitimacy of KSM's confessions is in question because many of his statements are the product of torture or abusive treatment.").

[263] *But cf.* Glazier, *supra* note 13, at 961 (noting that the World Trade Center was arguably a lawful target as an object "with a significant economic value").

[264] TAYLOR, *supra* note 56, at 628 (1992) ("It is true that, until Nuremberg, most of the trials based on the laws of war . . . were trials of military defendants. But I know of nothing in the laws of war that excludes unarmed civilians who violate the laws of war from criminal liability.").

[265] *In re* Yamashita, 327 U.S. 1 (1946).

[266] So, for example, Göring, the Reichsminister of Aviation, was indicted for war crimes, including murder and ill treatment of civilians, killing of hostages, and collective punishment of civilians, but nothing that resembled liability for any of the belligerency offenses committed against the Allies. The same was true of the other officers on trial, including Keitel and Jodl. I TRIAL OF THE MAJOR WAR CRIMINALS BEFORE THE INTERNATIONAL MILITARY TRIBUNAL, 14 NOVEMBER 1945 – 1 OCTOBER 1946, at 27-68. (1947).

violation of the law of armed conflict, one that the United States and its allies have punished in the past.[267]

A federal trial could allow for the denunciation of an evil breach of the gravest responsibility that a commission will not.[268] The federal court system, though not perfect, is unquestionably viewed domestically and abroad as both more fair and more open than a military commission. A trial in such a court, using existing rules of evidence and procedure, could not fail to both be and seem more just than a special court hobbled together for the purpose, particularly one that has already experienced so much chaos.

Ironically, the particular judicial defeats the United States has most recently suffered would not, by themselves, bar a trial of KSM. The attacks of September 11 constitute a grave breach, and KSM could be charged with liability for those offenses under the internationally accepted doctrine of command responsibility, even if the Bahlul opinion continues to prevent conspiracy trials as a violation of the constitutional separation of powers. It remains to be seen, of course, whether the U.S. Supreme Court will reverse the judgment of the D.C. Circuit that the Constitution limits military commission trials to offenses recognized by the international law of armed conflict. Even if the Court let that decision stand, however, there is little ground for the argument that the leader of the September 11 attacks, in deliberately targeting defenseless civilians, did not commit a violation of the law of war. Putting him on trial would not be a novel development.

The trial of General Yamashita at the close of World War II brings the point into stark relief.[269] His military commission trial was a litany of horror, as witness after witness recounted monstrous acts committed against a civilian population by Imperial Japanese

---

[267] The War Crimes Charge at Nuremberg included the allegation that "Frenchmen fighting with the Soviet Army who were captured were handed over to the Vichy Government for 'proceedings.'" *Id.* at 54 (Charge 3(c)).

[268] *But, cf.* Huq, *supra* note 13, at 1497 (arguing that the redundancy of having both military commissions and federal courts available is important to reduce the risk of inaccurate acquittals, or "false negatives").

[269] *See generally In re* Yamashita, 327 U.S. 1 (1946).

soldiers under his command.[270] No evidence showed that he directly participated.[271] The government did not even have evidence of a direct order for the atrocities.[272] Nonetheless, a panel convicted General Yamashita of liability as a commander for these grave breaches, as they presumably found it impossible to believe that he had not known or could not stop the behavior of his troops.[273]

In much the same way, a trial of KSM could focus on his responsibility for the September 11 attacks despite the fact that he was far away from these breaches. Evidence that he bore responsibility would fit logically under the command responsibility prong of liability. Even an international lawyer who rejected the

---

[270] *Id.* at 5 (noting that the commission heard two hundred and eighty-six witnesses). *See also* Danner & Martinez, *supra* note 36, at 123-24.

[271] A FRANK REEL, THE CASE OF GENERAL YAMASHITA 174 (1971) ("there was no finding of any order, any knowledge, any condonation on General Yamashita's part").

[272] During closing arguments, the prosecution appealed instead to a fire at a circus in Connecticut, after which employees were found guilty of manslaughter because they failed to prevent the loss of life. *Id.* at 165-66.

[273] *Yamashita,* 327 U.S. at 16 ("There is no contention that the present charge, thus read, is without the support of evidence, or that the commission held petitioner responsible for failing to take measures which were beyond his control or inappropriate for a commanding officer to take in the circumstances.") This treatment of command responsibility was the focus of the criticism of Justice Murphy, who argued that, in light of the lack of evidence of direct involvement by General Yamashita and the difficulties of maintaining control in the face of an Allied attack, the charges could be translated to:

> We, the victorious American forces, have done everything possible to destroy and disorganize your lines of communication, your effective control of your personnel, your ability to wage war. In those respects, we have succeeded. We have defeated and crushed your forces. And now, we charge and condemn you for having been inefficient in maintaining control of your troops during the period when we were so effectively besieging and eliminating your forces and blocking your ability to maintain effective control. Many terrible atrocities were committed by your disorganized troops. Because these atrocities were so widespread, we will not bother to charge or prove that you committed, ordered, or condoned any of them. We will assume that they must have resulted from your inefficiency and negligence as a commander. In short, we charge you with the crime of inefficiency in controlling your troops. We will judge the discharge of your duties by the disorganization which we ourselves created in large part. Our standards of judgment are whatever we wish to make them.

Id. at 34-35.

term "conspiracy" would nonetheless recognize this as command responsibility for the underlying offense.[274] She might well characterize it, in the language of the International Criminal Court, as ordering the commission of a crime which in fact occurred. But she would not reject a finding of liability for orchestrating the September 11 attacks as a peculiarity of the Anglo-American system.

Thus, defeats on the material support and conspiracy battlefields have, in truth, done nothing to harm the chance of an effective prosecution of KSM as an individual for his individual offenses. Those defeats, however, exist in the understanding of the public. Critics may use them as evidence of the flaws in the system. They have done significant damage to a military commission system already laboring under the burden of being perceived an extraordinary and unfair tribunal. A trial of KSM in a military commission could "succeed," if that term is taken to mean only that there would be a finding of guilt with an accompanying lengthy or even capital sentence.

If, however, success includes the educational function of a useful law of war military commission, failure in a KSM trial is foreordained. In 2003, such a military commission was possible.[275] More than a dozen years later, an ideological victory in such a forum is an impossibility. The only chance for global public education as a result of a trial of KSM exists in a federal court. If the defeats suffered by the government at the hands of federal courts in the cases of Hamdan and Bahlul lead the United States to trying KSM in a federal court, they will have been Asculum defeats indeed.

B. The Day After Tomorrow: Military Operations in an Alternate Universe

Whatever may happen with KSM, the United States has already won one victory by losing a series of cases. In military

---

[274] *See supra* Section II.B4(a).

[275] There would still have been opposition and objection, of course. *See e.g.*, Katyal & Tribe, *supra* note 62. That was nonetheless a very different world from the current one, in which a former Chief Prosecutor can write an editorial decrying the entire process. *See* Davis, *supra* note 256.

commissions as well as in the federal courts, the government has consistently failed to convince judicial authorities that belligerency offenses were properly subject to either a material support or conspiracy charge when tried by military commission. This position has frustrated some members of the government, several commentators, and a few dissenting judges. Their frustration over the short-term loss unfortunately causes them to miss the true significance of the catastrophic harm to U.S. interests that would have come with a victory.

Their displeasure is understandable. For centuries, military commissions have tried cases involving belligerency offenses that were nonetheless labeled violations of the law of war. In those cases, however, there was never a sense that liability extended beyond the individual. When General Washington convened a board of officers to try British Major John Andre, captured in civilian clothes after receiving the plans for West Point from Benedict Arnold, he was confident that it was legitimate to punish Andre for this behavior.[276] Like the Nazi saboteurs, it was the choice to remove his uniform that doomed John Andre. His protestations that he was a lawful member of His Majesty's Army were unavailing, because he was disguised as a noncombatant when he committed the acts in question.

Significantly, there was no sense—in 1780, or in 1942—that the liability for the offenses extended beyond the individual participants. Neither General Washington nor any member of his staff suggested that the British government had in some way violated international law.[277] The same was true of the German special operations branch that sent the saboteurs to the United States. They trained, armed, equipped, and transported the eight men to New York and Florida.[278] Yet, although six of the eight were themselves executed for their acts, no member of the German military hierarchy

---

[276] WILLIAM STERNE RANDALL, BENEDICT ARNOLD: PATRIOT AND TRAITOR 565-66 (1990).

[277] Indeed, General Washington himself employed spies. NATHAN MILLER, SPYING FOR AMERICA: THE HIDDEN HISTORY OF U.S. INTELLIGENCE 6 (1989) (noting that Washington "personally recruited agents, issued them instructions, and analyzed and acted upon their reports").

[278] O'DONNELL, *supra* note 86, at 21.

ever faced trial for the Quirin Group's sabotage attempt.[279] There was significantly more evidence against the leadership of the German high command, in this regard, than there was against General Yamashita.[280] The lack of a single trial evidences the broad consensus that committing a belligerency offense was an individual responsibility only.

This comparison of General Yamashita and the architects of the Quirin Group sabotage plans brings into stark relief the underlying distinction between grave breaches and belligerency offenses. In the category of grave breaches are those acts that individual states in the international community wish to see outlawed. Each nation is content that no nation should commit them, and each is thus willing to forgo any short-term advantage that might be gained through their commission. Such acts are so roundly condemned that jurisdiction exists everywhere and forever.[281]

If there is an international agreement on belligerency offenses, it is the opposite one. Each nation wishes to maintain the ability to punish individuals who seek to harm it, and reserves the right to try those who do not possess proper combatant immunity. On the other hand, virtually all nations wish to preserve the freedom to operate in such ways by themselves. Most nations around the globe maintain official spy agencies, despite exemplars like John Andre. The fact that individual members of such agencies are subject to punishment, even capital punishment, does not deter nations from training and deploying such people.

Likewise, many governments wish to continue supporting unlawful combatants in missions of belligerency beyond mere spying. From Iran's support of Hezbollah[282] to the United States'

---

[279] *Id.*

[280] Reel, *supra* note 271, at 160-61 (recounting the defense argument that the destruction of communications in the Philippines made it impossible for General Yamashita even to know that atrocities had occurred).

[281] Kenneth C. Randal, *Universal Jurisdiction Under International Law*, 66 TEX. L. REV. 785, 810-15 (1988) (discussing the trial by Israel of Adolf Eichmann).

[282] Jenco v. Islamic Republic of Iran, 154 F. Supp. 2d 27, 31 (D.D.C. 2001) ("the Court also finds that The Islamic Republic of Iran and the Iranian MOIS [Ministry

support for the Contras in the Central American wars of the 1980s,[283] nations frequently find it in their interests to arm, train, and assist civilians who undertake violent activities without the legal shield of combatant immunity.

Indeed, the United States, despite pressing vigorously at military commission trials for responsibility for belligerency offenses, maintains an interest in promoting a robust series of such behaviors. An entire unified command, the United States Special Operations Command, exists to train and operate non-conventional forces.[284] Although many of the units of this command comply with all of the ordinary rules of uniform wear during armed conflict, many others do not.[285] Soldiers and sailors in civilian clothes operate as if they were part of a civilian noncombatant population. Those men and women are well aware that they are individually subject to prosecution for belligerency offenses, as Hicks and Hamdan were.[286] There is no expectation, though, that their trainers and supervisors at the Pentagon, or the White House, are subject to liability for employing them in pursuit of national objectives.[287]

---

of Information and Security] provided support, guidance, and resources to Hizbollah").

[283] John Norton Moore, *The Secret War in Central America and the Future of World Order*, 80 AM. J. INT'L L. 43, 72 (1986).

[284] 10 U.S.C. § 167 (2014).

[285] W. Hays Parks, *Special Forces' Wear of Non-Standard Uniforms*, 4 CHI. J. INT'L L. 493, 498-99 (2003) (noting that in the Afghanistan conflict the "Commanding General made the uniform decision, favoring civilian clothing over DCU [Desert Camouflage Uniforms]. His rationale was based on two factors: (a) the ability of soldiers to perform humanitarian assistance operations; and (b) the safety of Civil Affairs personnel--that is, force protection.").

[286] SOLIS, *supra* note 47, at 224 (describing examples of the practice of fighting in civilian clothes from the First World War to the U.S. war in Afghanistan and concluding that "Commanders will continue to order subordinate combatants behind enemy lines to fight without uniform or distinctive sign and, knowing the risk, subordinate combatants will willingly comply).

[287] Indeed, some commentators have argued that not all wear of civilian clothes by combatants even violates the law of armed conflict. *See, e.g.*, Parks, *supra* note 285, at 523 ("State tolerance of Special Forces' fighting in civilian clothing is limited to special circumstances, such as support for partisans, which is consistent with humanitarian tolerance for captured guerrillas."). Even if Col. Parks is correct,

Yet there would be such liability had the United States succeeded in the rewriting of the law of armed conflict so vigorously pursued by the prosecutors of the military commission. If such a tribunal, adjudicating violations of international law, has jurisdiction to pronounce sentence on those who conspired with unlawful belligerents—or worse, those who "materially supported" organizations opposed to the adjudicating nation—then a whole new form of liability would develop. A type of behavior participated in by many nations, including virtually all of the great powers, would suddenly be the subject of criminal prosecutions.

The idea of high ranking American military officers, or even senior political officials, on trial for deploying special operations forces is one grotesquely at odds with a broadly held consensus, at least among government officials, on what behavior the United States should participate in.[288] Yet the only argument that could be deployed against such trials is the notion that something special about the United States elevates it above the rules that bind the rest of the international community. If that is the meaning ascribed to the term "American exceptionalism," it will only result in increasing global hostility and a desire by other nations to frustrate American objectives. If a criminal system outlaws behavior not on the basis of what is done, but on who does it, the system will be untenable unless supported by a ruthless hegemony.[289] The United States does not exercise that kind of hegemony in the world, nor should she, nor should any nation.

V. RETURN TO TOMORROW: HOW THESE LOSSES HELP THE GOVERNMENT

At the beginning of the 21st century, the United States found itself in a troublingly novel position. Global events and quickly-

though, it is notable that even the cases of wear of civilian clothes that he would consider perfidious have not created liability for inchoate crimes.

[288] *See* Frakt, *supra* note 35, at 751 (noting the explanation by Harold Koh, Legal Advisor to the State Department, that criminalizing all civilian participation in hostilities could not be reconciled to the CIA's drone program).

[289] TAYLOR, *supra* note 56, at 641 ("There is no moral or legal basis for immunizing victorious nations from scrutiny").

made decisions left the United States holding a large number of foreign citizens with little precedent to guide in the ways in which they should be handled. The rhetoric of endless war and their own great evil—they were, in the words of the Secretary of Defense, "the worst of the worst"[290]—blocked the logical step of treating them as if they were among the many ordinary prisoners of war and temporarily detained civilians that the military had experience in dealing with.[291] An answer of sorts was found in the quirky, malleable history of the military commissions.

Unfortunately, most of those held by the United States were utterly unsuited for a role in a useful, educational military commission. With only a handful of exceptions, the detainees were much more analogous to ordinary foot soldiers performing ordinary acts of combat. It may be that combatant immunity did not protect them from the legal consequences of firing weapons at invading soldiers, but it was unlikely that the world community would develop any sense of outrage about their behavior.[292]

Eventually, most of the detainees were simply released. Most of those releases were accomplished with no fanfare, and little public attention. This may be part of the reason that a significant percentage of the American people continue to wish the detention

---

[290] Randall T. Coyne, *A Law Professor's Reflections on Representing Guantánamo Detainees*, 1 NE. U. L.J. 97, 98 (2009).

[291] In addition to the millions of prisoners of war whom the U.S. has detained throughout its history, the military had recent experience in conducting the tribunals mandated by Article 5 of the Third Geneva Convention to determine whether a particular person was entitled to prisoner of war status, and hence protection from prosecution for belligerency offenses. *See* Robert M. Chesney, *Iraq and the Military Detention Debate: Firsthand Perspectives from the Other War, 2003-2010*, 51 VA. J. INT'L. L. 549, 562 (2011) (noting that United States conducted almost twelve hundred such tribunals during the Gulf War in 1991).

[292] Consider, for example, the Canadian response to Omar Khadr: he has now not only been released on parole, but a judge ordered the removal of his electronic monitoring ankle device, apparently accepting his argument that it "was embarrassing and interfered with activities such as biking, swimming and playing soccer." *Judge Eases Omar Khadr's Bail Conditions, No Monitoring Bracelet*, THE GLOBE AND MAIL (Sept. 18, 2015).

facility at Guantanamo Bay to remain open.[293] A few detainees, like the Louisiana-born Yasir Esam Hamdi, became the subject of media focus, which created a certain dissonance between the language of the government and the ultimate conclusion of the detention story.[294]

A few detainees, however, were men of substance, men who had played significant roles in the grave breaches committed in the name of Al Qaeda. For these men, a prompt and open military commission might have taken on the role of Nuremberg, educating the world about the logical and horrible end result of that ideology. Such military commissions never happened; the government chose instead to start with small players, to test the system in a series of trials of belligerency offences. In almost all of those cases, even the ones that seemed to be government victories at the time, the United States effort to conduct trials by military commissions have ultimately ended in defeat.

In order to get convictions in those cases, the government attempted a dramatic revision of the law of armed conflict. In the only real paradigm case, that of the Nazi saboteurs, the prosecution was aided by an informant within and a large amount of easily handled physical evidence. In cases like those of Hicks and Hamdan, the government felt sufficiently ill-at-ease about the result that they resorted to novel twists. The introduction of material support as a charge was one such twist, and it resulted in a quick and severe Asculum defeat.

The use of conspiracy for belligerency offenses was defeated in a similar fashion, and the ramifications of that loss will redound to

---

[293] PEW RESEARCH CTR., *Obama Job Rating Ticks Higher, Views of Nation's Economy Turn More Positive* (Jan. 14, 2015) ("More Americans think closing the prison in the next few years is a bad idea (49%) than say it is a good idea (42%).").

[294] *Compare, e.g.*, Brief for Respondent at 4-5, Hamdi v. Rumsfeld, 542 U.S. 507 (2004) (No. 03-6696) (noting that only detainees with "a high potential intelligence value or pose a particular threat" would be transferred to Guantanamo Bay, and that Hamdi was one of those transferred) *with* Press Release, Mark Corallo, Dir. of Pub. Affairs, U.S. Dep't of Justice, Regarding Yaser Hamdi (Sept. 22, 2004) (announcing the release of Hamdi to Saudi Arabia after the Supreme Court ruling in his favor with the observation that "the United States has no interest in detaining enemy combatants beyond the point that they pose a threat to the U.S. and our allies").

the benefit of the United States for years. Initially, if the collapse of military commissions as a reliable way of adjudicating guilt reduces congressional opposition, it might allow a federal trial of KSM. A trial of KSM in a forum recognized internationally for both legitimacy and dignity presents the best remaining option for a useful, educational airing of the extent of Al Qaeda's horror. A trial of KSM in a military commission in 2003 might well have had a similar result, but that forum is now so damaged that any sentence from one would be tainted with illegitimacy and might well merely foster recruitment for Al Qaeda and other extremist groups.

The spectacle of American leaders being called to answer for the new "crime" of training and deployment of spies and irregular forces would be a strategic defeat. It, too, is made less likely by the smaller setbacks of the early military commission trials. A world in which the community of nations has agreed to outlaw participation in irregular warfare, as it has agreed to outlaw the torture of prisoners of war, is not necessarily a bad one. The nations of the world have not consciously considered and discussed the creation of such a world. The short-term thinking of one great power should not seek to bring it into existence.

VI. CONCLUSION

The desire to convict every battlefield opponent of the United States of a belligerency offense was misguided. The plan to use the military commissions for that purpose was ill-conceived. The series of small defeats that arose from a misunderstanding of the history and nature of military commissions, however, prevented a far greater strategic defeat for the long-term interests of the United States. There remains the possibility that a public trial of those involved in the commission of grave breaches will improve the standing of the United States in the world community, and prove to be a rallying point for the use of law to combat terror. If that happens, little credit will probably be given to the course of failures that made eventual success possible. When we look back at the story of King Pyrrhus, the drama of his situation causes us to focus on the victory that offered him little solace. For Hicks, and Hamdan, and Khadr, victory does not erase the years spent in difficult situations as

a detainee. Those who think of Pyrrhus' eponymous victory, however, should give a thought to Rome's rise to power. Without their defeats, the Romans could not have conquered. Without the military commission losses, the United States would be in a far worse position, both today and tomorrow. Indeed, one "victory" at such a proceeding might have utterly undone the nation.

SYMPOSIUM PANEL

POLICY BY OTHER MEANS:
A REVIEW OF DOD'S LAW OF WAR MANUAL

Matthew McCormack, Dr. Nicholas Rostow, & Tom Bowman*

On November 16, 2015, the National Security Law Journal *at George Mason University School of Law hosted* Policy By Other Means: A Review of DOD's Law of War Manual*, a symposium featuring a panel discussion on the Department of Defense's Law of War Manual, which was released in the summer of 2015. Following is an edited transcript of the remarks.*

RICK MYERS, EDITOR-IN-CHIEF: Thank you for coming tonight. My name is Rick Myers, and I am the Editor-in-Chief of the *National Security Law Journal*. I want to welcome you to our Fall Symposium, "Policy by Other Means: A Review of DOD's Law of War Manual." The Law of War Manual was just released this past summer; we're excited to present this discussion today.[1]

---

* Matthew McCormack, Associate General Counsel in the Office of General Counsel for the Department of Defense; Dr. Nicholas Rostow, Professor at National Defense University; Tom Bowman, National Desk Reporter for National Public Radio. The panel was moderated by Harvey Rishikof, former Chair of the Advisory Committee, to the Standing Committee on Law and National Security.

[1] This article is an edited transcript of remarks delivered on November 16, 2015, at the *Policy By Other Means: A Review of DOD's Law of War Manual* symposium hosted by the *National Security Law Journal* at George Mason University School of Law in Arlington, Virginia.

As you can read in your program, the *National Security Law Journal* is one of the student-edited journals here at George Mason University School of Law. We publish two issues a year. Volume 4, Issue 1 should be available in the upcoming weeks. In the meantime, I invite you, if you enjoy the debate and discussion today, to visit our website, nslj.org. You can find all of our past volumes online as well. At this time I would ask you turn off or silence your cell phones and any electronic devices. Your program also has a detailed [biography] for each of our panelists and our moderator that you can read.

At this time, though, I'll introduce our panel. At the end [of the table], we have Dr. Nicholas Rostow, who is a professor at the National Defense University. Next to him is Mr. Tom Bowman who is a National Desk Reporter for National Public Radio. Next to him is Matthew McCormick who is Associate General Counsel in the Office of General Counsel for the Department of Defense ("DOD"). And then finally, our moderator tonight is Mr. Harvey Rishikof, who is Chair of the Advisory Committee, to the Standing Committee on Law and National Security. So, at this time, I'll turn it over to you Harvey.

HARVEY RISHIKOF: Thank you so much. Let me first thank you, Kirstin, and the school for putting this together. It's a wonderful panel that we've been able to assemble, and I notice some great luminaries in the audience who we will expect to have fascinating questions from and the rules of engagement are, is it our expectation that the journal may be editing the discussion and may publish it so we may want to include the questions posed from the audience, so I encourage you to be concise and brevity is the soul of wit when it comes to a question. But you will probably be recorded as part of the proceedings this evening.

I'm not going to go into the bios of the individuals. I know most of them extremely well, and I think they're going to [have a] fun conversation, but as you know the document is [1,172] pages with [allegedly] 6196 footnotes. That's how you know there may have been one or two lawyers involved in the production of this extraordinary document. But I think this is the first night that we're going to start debating and around town, there are going to be a lot

of conferences trying to analyze this document from a whole variety of perspectives. But I want to compliment Matt as representing the DOD tonight for—this is a long awaited document, and hats off go to you and . . . Stephen Preston who [helped] manage [to] get this baby out the door.

So with that, what we thought we would do was let Matt set the table for a few minutes and then we thought Tom might have one or two issues or questions concerning the reporter section of the Manual and then Nick, as a professor of International Law will . . . raise some of the [major] theme[s] and big issues that we see in the document. So with that, Matt take it away.

MATTHEW MCCORMACK: Ok, thank you, I appreciate it. Well thank you to the *National Security Law Journal* for also inviting me to be here this evening. Before I begin, I have to mention that the views expressed tonight are my own and don't necessarily reflect the views of the United States Government or DOD. So with that caveat, let me begin with some background about the Manual.

MR. RISHIKOF: I think we'll have the caveat for both you and for Tom vis-a-vis NPR [and] Nick . . . for DOD. All the caveats in place, so you are not speaking for your organizations, including myself. So you won't have to do that, okay? For the record.

MR. MCCORMACK: Thanks. So, just over five months ago, the Office of General Counsel for DOD published the DOD Law of War Manual, which is the first ever department-wide Law of War Manual.

My original plan for our talk this evening was to begin to summarize the 1200 pages for you; they told me I only had ten minutes so you know that plan went out the window.

[AUDIENCE LAUGHTER]

So, my plan this evening, to your benefit, will be much more modest. I'm simply going to make a few remarks about what the Manual is, who wrote it, why it was written and how we envision it being used. While doing so, I'll also explain what the Manual is *not* which oddly enough can actually help people better understand the Manual's purpose and design. So first and foremost—what is this DOD Law of War Manual?

The Manual is an informational publication about International Law, more specifically, the law of war. The Manual is not directive in nature; it is descriptive in nature. The U.S. military, like so many other militaries in the world, works through a system of affirmative domestic authorizations, and orders given by civilian authorities. Thus, even though those orders [and operations must] comply with the law of war, the authorizations for taking those actions are domestic orders, not the law of war, much less an informational Manual about the law of war. In any event, the law of war is mostly prohibitions and restrictions and imposes obligations if certain actions are undertaken—it doesn't authorize or tell military forces or anyone else how to prosecute a military campaign or how to really act in war. Thus, legal discussions in the Manual about [how] the law of war deals with certain issues such as "What constitutes spying?" or "Under what circumstances may a person be entitled to treatment as a POW?" is not an authorization for US military personnel to take any particular action. It just describes legal rules and resulting legal consequences of taking certain actions.

So the Manual describes U.S. international legal obligations. The Manual doesn't create or change any law, either international or domestic, or create or change any policy. So, when you look closely at the Manual, you'll see that it's largely written from a retrospective perspective. The Manual largely takes existing treaty obligations, existing interpretations of legal rules, and other existing legal positions that the United States or DOD has taken.

We thought that a retrospective approach would be the most beneficial approach for the primary audience of the DOD Manual, which is DOD legal practitioners. The most important thing for the start of any new legal analysis, is what was the last official authoritative U.S. or DOD-level position on the subject? Not an

abstract position crafted solely for the purpose of drafting a manual or even to advocate for a change in the law. Some people may dislike this retrospective approach because they want something more aspirational. Other people, such as practicing DOD lawyers, should really find the approach that we took useful.

So, it should go without saying that the DOD Law of War Manual was not drafted to codify customary international law ("CIL"). Even though the Manual refers to customary international law, the Manual focuses on the law of war applicable to the United States regardless of its source. So even though the Manual addresses CIL, not everything in the Manual is an expression or reflection of CIL. For example, the Manual states treaty rules, [and] U.S. law and policy [in some cases]. So it wouldn't be correct simply to take statements in the Manual and say that the Manual reflects DOD's views on CIL. By contrast, scholars have sometimes used military manuals in this way and the United States has objected to that. That said, when [the] U.S. legal position's was that some rule does reflect customary international law, we said so in the Manual.

Now the Manual was prepared at the direction of the Secretary of Defense, by what we call the Law of War Working Group, which is chaired by a representative from the Department of Defense's General Counsel's Office. Over the last five years, that has been my boss, the Deputy General Counsel for International Affairs, Chuck Allen. The Working Group also includes representatives of all the service branches Judge Advocates General and [Military Department] General Counsel, as well as the Staff Judge Advocate to the Commandant of the Marine Corps, and [the] Legal Counsel to the Chairman to the Joint Chiefs of Staff. We're also grateful to have received input from colleagues from the Department of Justice and the State Department. Of course, within my office, there was a very small team of lawyers who were researching and writing the text, chief among them, Karl Chang who was the principle drafter of the Manual.

Even though this is the first DOD-wide manual on the law of war, this is not the U.S. military's first statement about the law of war. As noted in the foreword to the Manual, General Washington directed that the Continental Army would follow the law of war.

And then during the Civil War, President Lincoln issued General Order Number 1[00], the famed Lieber Code, which provided the basis for similar regulations in other countries and early multilateral treaties on the law of war. Throughout the twentieth century, each of the Military Services has issued multiple pamphlets and manuals on the law of war. So publishing this DOD-wide Manual is just the next step in DOD's effort to disseminate information about the law of war to its forces.

And this brings me to the issue of how we envision [the Manual] being used. Of course, some may wish to read it from beginning to end: I would not recommend that *[humorously]*. [More seriously,] we [can] see the Manual being used by instructors in the law of war, both civilian and military. But really, first and foremost, the audience that we had in mind was the DOD legal practitioner. We envisioned the Manual being used as a reference work for the practicing military lawyer. So, for example, a military lawyer who is advising an operational commander would use his or her Manual to refresh his or her knowledge of a particular rule. The practitioner would use the Manual [to] find the particular rule at issue, and the relevant U.S. and DOD interpretations of that rule. The Manual also identifies sources where further information can be found. With the practitioner in mind, we largely wrote the Manual with the rule stated up front and clear.

This leads me to my last point: the Manual's online nature and it's design, which oddly enough—the fact that it's electronic—[has been the] subject [of some] controversy. People have expressed a lot of opinions about [it being] an online, electronic manual rather than a bound version . . . . But, before you hit "print", or before you spend $75 and send it to LawofWarManual.com, let me make a pitch for why [we believe that an electronic publication has distinct advantages over a printed version]. Really, first and foremost, the primary advantage for DOD, was that an online Manual would be immediately accessible. You post it and it's not just accessible within DOD, but anybody in the world can hit [the website] and look at [the Manual]. And, the second thing we realized was that we would be periodically updating [the Manual]. Of course, the law isn't static. So, we can envision updating the Manual on a periodic basis. [With an electronic Manual, no one is left] referring to version 1.0 after [we

have updated successive editions of the Manual for] ten years and we're now on version 6.0. That's unless you printed it out, or you spent your $75.00 [to buy a copy from LawofWar.com] *[humorously]*. So, [these are some] of the reasons for having an online Manual [and] why that makes sense to us.

[Also, an] electronic Manual is just eminently easier to navigate and use for a legal practitioner. For example, you're able to have Manual-level and chapter-level tables of contents that are hotlinked. We were able to have footnotes that [are] cross-linked to other sections. If you'll notice, the Manual is drafted largely in chunks of information. Those chunks of information have a descriptor that allows it to be identified so that it can be used as a cross-reference in the footnotes so that you don't have to repeat a lot of the same information over and over again in the Manual as you're building ideas or just wanting to discuss one topic. Without the ability to easily cross-reference other information, the Manual would have been ten times longer than it is *[with exaggeration]* because so much of the law of war is interrelated.

Some of the other features that really help with an electronic Manual are that Adobe Acrobat has section bookmarks, which is a table of contents that runs along the left hand column and other features. And, maybe the most powerful or most obvious [feature] is the ability to word-search—being able to plug in a word and find it immediately is just incredibly powerful for the researcher or a user of the Manual. Maybe just to draw one quick example: I picked a phrase, "Martens Clause." How long would it take for me to find information by just opening the "find" button and typing it in? It took four seconds. Really all I did was typed it in, [and] it went to the first place it was mentioned in the Manual, which was in Chapter 2. There's a footnote there that says "Refer to section 18" "blank blank" section, "Martin's Clause." I hit that [cross-reference], and there I have the information I was looking for—the Martens Clause. Now, without the ability to use the electronic cross-referencing, you would have to have a much more sophisticated understanding of how the Manual is organized, and then a much more sophisticated understanding of the law of war. For instance, there is nothing in the Table of Contents that says "Martens Clause," right? And, we also didn't index the Manual because it would take a professional indexer

to do that and so we would still be waiting for the thing to be indexed if we were to go that route. So the Martens Clause information is included under the 1899 and 1907 Hague Conventions . . . because that's where the Martens Clause first appeared. But, unless you already knew that, you would have had a tough time finding it; you might've looked in ten different places. The other thing [to note] is that information [on the Martens Clause] is on page 1,173 in Chapter 19 *[with exaggeration]*. You would've spent a long time looking for it and you just don't have that issue with [an] electronic Manual.

MR. RISHIKOF: Just for the record though, it's actually [1145].

MR. MCCORMACK: [1145]—I just made [the number 1,173] up [for effect].

MR. RISHIKOF: But that, again, this is just for the printed version

MR. MCCORMACK: How'd you know that? How'd you know the Martens Clause—you looked for it—you looked for it, too?

MR. RISHIKOF: I did.

MR. MCCORMACK: How about that? *[rhetorically]*

MR. RISHIKOF: We did not plan this, but I knew the Martens Clause would come up in the discussion, so I looked it up.

MR. MCCORMACK: Really?

MR. RISHIKOF: Yeah, but so, that's a perfect example—

MR. MCCORMACK: You worked for the Intel community at one point.

[AUDIENCE LAUGHTER]

MR. RISHIKOF: I've worked for many communities, but let's continue.

[AUDIENCE LAUGHTER]

MR. MCCORMACK: So, one last thing, we've heard people say, "I want something I can put in my pocket." [With the Manual], you can download it to your laptop or iPad and you're off and running.

Now, to say that we published the Manual is not to say that we are done with the Manual. We've already begun looking at ways to improve it. So, if you have thoughts about that, I'm going to be taking notes tonight. I [also] have colleagues in the audience who will be taking notes. The preface [of the Manual] also includes an email address where you can send comments. We encourage you to do so. That would be super helpful for us. When you do provide comments, try to make them as detailed as possible. If it's a legal source that you believe that we missed, or some other state practice that's otherwise not mentioned that you believe would be helpful, that would be very welcomed. So with that, I'll end my remarks and thank you for your attention.

MR. RISHIKOF: First of all, there are a number of things that are quite fascinating about this because, for the academics in the audience, though this exists, the authoritative version is going to be electronic.

MR. MCCORMACK: That's correct.

MR. RISHIKOF: So before you cite this as the authoritative version, all the academics have to go to the electronic site to make sure it has not been changed.

MR. MCCORMACK: That's correct.

MR. RISHIKOF: Which I've never—that's a really quite amazing phenomenon.

The second thing is, you said, "This Manual does not however preclude the Department of Defense from subsequently changing its interpretation of the law. Although the preparation of this Manual has benefited from the participation of the lawyers at the Department of State and the Department of Justice, this Manual does not necessarily reflect the views of any other department or agency of the United States Government or the views of the United States Government as a whole." That's also quite fascinating in this particular section. And then finally, the cover, you can't see, but it is a picture, I assume. I'll have to look at the citation because Senator McCain is on the cover as a POW. And just for the record, there is a guy that looks a lot like you behind them, but I'm sure it's not you given your age.

[AUDIENCE LAUGHTER]

MR. MCCORMACK: Yeah, there is an age difference I think.

[AUDIENCE LAUGHTER]

MR. RISHIKOF: . . . It is fascinating, the cover, is the current Senator who is Chairman of the Senate Armed Service Committee. With that, Tom . . .

TOM BOWMAN: Okay.

MR. RISHIKOF: I think there might be some issues that you specifically want to raise?

MR. BOWMAN: Sure.

MR. RISHIKOF: Then, we can move forward. But we thought it might be interesting if you might be able to comment on a section you find personally interesting.

MR. BOWMAN: Sure. I want to state from the outset, I'm not a lawyer, nor have I trained to be a lawyer, like many of you fine people out there. I am looking at this strictly from the position of a journalist—I've been a journalist all my adult life. And, I first became aware of this, the New York Times did an article on it a few months back and I did like I always do, everyday, I posted [it] on my Facebook page. And immediately, I got a response from a Marine Colonel I spent a lot of time with in Afghanistan, and it said, "Tom, you know nobody pays attention to manuals, why are you even putting this up there?"

Alright, so I didn't think too much of it until National Public Radio wrote a letter, a senior official at NPR wrote a letter. It says [reading from the letter], "Dear Secretary Carter, A country that protects its journalists, protects the truth. The Department of Defense recently released Law of War Manual fails to do that." So then I said [to myself], "Wow, I should look into this a little more, since my bosses have just written this letter to Secretary Carter."

So, not being a lawyer, but knowing some great lawyers, I sent a note to Gary Solis who was a Company Commander in Vietnam, then became a JAG, [and] taught law at Georgetown and George Washington. So I sent Gary a note. I said, "Hey Gary, what do you think of this new Law of War Manual?" [Reading from letter] "Tom, Oh yes, I've looked into the new Law of War Manual, as some of my fellow law of armed conflict teachers have. This Manual is not good. I admit, I've read only bits and pieces of it, but who can say they've actually read it? It's too long for anyone with a life to have read it. More significantly, it's only available online, discouraging any coherent study of its contents, and it has no index." So, when I see Gary, he's going to get a copy of this right here. I'm going to make sure he gets it. He's going to have to carry it in his rucksack, but he will get a copy. So it's a nice long note from Gary, and he said his concern is, it's nothing like any LOAC Manual previously published by the U.S. "I have all the antecedent Manuals, the first dated 1914, the latest antecedent Manual issued in 1956 is 192 pages of text. A bunch of it simply repeating the 1949 Geneva Conventions." And he said—goes on to say that—you know the whole issue of an unprivileged belligerent, which I guess I could become at some point overseas in the field—I've been called a lot of things in my life, worse than this, but this is pretty grim—unprivileged belligerent. Now, Gary Solis says, "It's generally accepted that an unprivileged belligerent is 'a civilian who takes up arms and directly participates in hostilities.'"

So one of my questions would be, well, why would anybody call me an unprivileged belligerent for reporting on the news? I just didn't get it.

So I looked into it further and the Committee to Protect Journalists delved into this a bit and talked about what the Pentagon expects you to do. It says, first of all, "to avoid being mistaken for spies, journalists should act openly and with the permission of relevant authorities." Which is problematic for how we do our work—some of our reporters have gone to Syria and Libya. They didn't ask permission of Gaddafi or Bashir al Assad to go there. So, that's a serious problem—and a lot of times we do not act openly. We're prof . . . well, we're not professionals. We've been down this road before, it's really a craft. But we can talk about that later. But

you always want to say, "Listen, I'm doing a story, my name is Tom Bowman." With anybody you meet—whether it's a villager in Afghanistan, or whether it's a United States Senator, you always want to be open about who you are. But *acting* openly is different.

Now, sometimes we're out with military in Afghanistan and I might take a little side road and talk with some villagers about what they really think about what is going on. And, I was just there in April and in May talking with—I imbedded with the Afghan forces for a month which was fascinating and we would take villagers aside and say "What do you think is going on here?" And this poor old guy said—and I didn't ask permission of anybody to do that, I mean that's not how we do our work. And I said, "Well, what do you think about what's going on?" He said, "Listen, I live in this little village. Every time I go out and try to tend to my cow, I get shot at by the Afghan forces. They come in, talk to me, and then, that night, when they leave, the Taliban comes in and beats me up for talking to the Afghan." That tells you what is going on in that country. But I'm not going to go up to the Afghan officer and say, "Do you mind if I just talk to this guy?" Because he's probably going to say "no."

So we're open in who we are and [in] describing who we are, but sometimes we do not act openly. And again, permission of relevant authorities is clearly problematic for the world we live in today. We had one of our reporters, Kelly McEvers, bravely—one of the bravest reporters I know—go into Syria wearing a burka. And if she got caught, she'd be in serious trouble.

It's actually easier for a woman to go because she could sit in the back seat. If a guy goes, clearly I do not look like a Syrian, I would not pass, so I would have troubles. But she could sit in the back seat. She didn't ask permission of anybody. Some reporters to this day go through the government channels and they go to Damascus and go around Damascus and they're taken around by minders and that's not how we like to do our work, having a government minder sitting with us. So, I find that to be particularly problematic.

And, then it goes on to say that "States may need to censor journalists work or take other security measures so that journalists do not reveal sensitive information to the enemy." That's a loaded

term—"sensitive information." What is "sensitive information?" Now, I know if somebody slips me a top-secret document, that's clearly sensitive and somebody may go to jail . . . or if someone gives me signals intelligence, which is highly classified. If Matt gives it to me, and of course he never would, but Matt goes to jail and I could potentially go to jail, right? 18 U.S. Code 1798. As Bobby Ray Inman said to me many, many times when I talked to him many years ago.

So, but sensitive information could be anything. And I'll tell you one thing, this day and age, I don't want to mention any names or administrations, but this is a particularly closed administration. They put out a letter two years ago that any general officer that meets a reporter informally has to tell authorities—public affairs—that "I met Bowman at a backyard barbeque." They don't reveal much about causalities among Afghan forces—they consider that sensitive—but, it doesn't tell you how things are going. We had a general who said that the casualties in Afghanistan, said at a Pentagon briefing that "casualties are unsustainable," and they bit his head off. They don't want to tell you what's going on—they consider all that sensitive. So if I print that stuff, do I run afoul of this stuff? Is someone going to put me in handcuffs? Is someone going to throw me out of Afghanistan or throw me out of an embed?

This happens time and time again when we do our work. The Marines in Afghanistan never reveal the specifics of a Marine casualty. A Marine may die in Helmand Province. They won't tell you where it happened or what the circumstances were—they consider all of that sensitive information. The Army will say, "We lost a soldier North of Kandahar in an IED attack or a complex attack," they'll reveal it—the Marines will not.

So, if I'm out with the Marines and I broadcast that, "Poor Sargent Jones died in a complex attack from an IED and then was shot afterwards," is that sensitive information? Can I run afoul of this? So, I see this time and time again when I'm looking at this as well.

Also, you know when I was in Iraq, I interviewed a guy that was a soldier with the Mahdi Army—he was the enemy of the United States. And one of our translators said, "Do you want to sit down with this guy?" I said, "Sure." So, we walk down the street. We leave

our compound, which had blast walls around it. We hop in his car. We drive away to a parking lot where we meet another guy. We hop in his car. And, this guy's driving away. Drives to an abandoned building in the outskirts of Baghdad. Big concrete building, water dripping, dark. And, I walk in there and I said, "This is probably the dumbest thing I've done in many, many years." And, the guy who's driving the car turns to me and says, "I'm sorry we had to meet this way. But, I am the Mahdi Army Commander. Would you like some tea?" I said, "I would love some tea."

Now, clearly, I could run afoul of these rules and regulations by meeting with that Mahdi Army guy. And also, you know, the Sons of Iraq. They were shooting at American forces and all of a sudden, then you're paying them 300 bucks a month. Now, if I talk to this guy before you start paying him, do I violate these rules? And once you cut him a paycheck, it's okay for me to talk with him? I don't get it.

So, you know, this is the way we do our job. We have to get out there. We don't ask permission of anybody. I get it; if I'm imbedded with U.S. forces, there are rules and regulations—I believe too onerous, but that's another story—I'm prohibited from talking to anybody wounded unless that person gives permission. I'm prohibited from taking pictures of the dead with any markings. I once tried to get—we were in a firefight in an attack by the Taliban—a roadside bomb blew up a 40-ton striker vehicle, flipped it over, killed a couple of guys. They put them in a body bag and I took a picture of the body bag. I almost got beaten up by the Sergeant. He said, "You're not supposed to do that." I said, "Hang on a second. The rules say 'No pictures of the dead.' This is a body bag." But, it could have gone either way with this guy, right?

So our jobs are hard enough as they are, doing this day [in] and day [out] without having this kind of thing—without being called unprivileged belligerents, without saying this is 'sensitive information'—I'm telling you right now, we already have a hard enough time getting *any* information. So that's what troubles me.

And Matt's a good guy, we had a discussion earlier, but one of the other issues that NPR has was that you basically say that "Information that could be shared with a hostile force," and NPR

said, "Hang on a second. How about information shared *only* with a hostile force? Why don't you change the language?" And the Defense Department said, "Yeah, we'll look into that." And NPR also said, "Did you ever sit down with any journalism groups, any journalists to walk through this stuff before you did it? That would have been helpful." They said they would take that under advisement. And I hope they do sit down with them and go through some of this stuff because you know some of it's troubling in how we do our work and also, the concern that NPR has and other journalists is, you know, someone is going to look at this Manual and see "unprivileged belligerent" in some more repressive government and say, "Wow, this what the United States is saying. This is what they're putting in their Manual. We can do anything we want. We can be even harder on our people. And justify it—sensitive information." So, those are some of my concerns on it, I hope they would at least talk to journalism groups and deal with this in a more serious way. But, those are some of my concerns. I'll stop there. We can . . . talk about this in the Q&A, but again, I just think on review of this, there are some problems.

MR. RISHIKOF: I may change the rules and let you engage immediately, but let Nick speak but we clearly have engagement. And, as you know, this is one of the issues when the Manual came out that a lot of people are . . . focusing on so I think we look forward to having an interesting discussion about the complexities and nuance about what this means as you interpret the DOD [Manual]. Nick—

DR. NICHOLAS ROSTOW: Thank you, it's a pleasure to be here and share this platform with such distinguished personages. And, I want to thank in particular, the *National Security Law Journal* for inviting me. Harvey has kindly taken care of the disclaimer; we can assume it was made. This is a beast. I've been on record as an enthusiastic supporter of the effort to write [the Manual] and to get it out, and I still am.

But, I will be candid in my comments because the kind of thing that Tom has just highlighted is not unique to the section on

Journalists. First of all, the question demanded by the title is, "Is it a manual, really? Or is it a treatise?" Either way, it may not be the official statement of the U.S. Government but it in fact is. And nothing like it exists anywhere else in the U.S. Government; nothing like it has ever been published by the U.S. Government. It is not analogous to the hundred and fifty page document produced by the Army in the 50s or the Navy subsequently, and it is therefore, uniquely important and uniquely valuable.

I say uniquely important because for years it has been in the making. I don't [think] that Matt, you said exactly how long it had been in the making, but I know [that] Hays Parks—probably the most distinguished single expert on the laws of war in the United States for many, many years worked on this and couldn't bring it to conclusion before he retired—first as a Marine and then as a civilian.

And it is of enormous importance *because* it is the U.S. Government's statement on the laws of war. And the entire international community has been waiting for it. [Everyone] knew it was being worked. There were experts from foreign countries who participated and read [earlier] drafts and commented on drafts and the International Committee of the Red Cross, which arrogates to itself the chief interpreter of the Geneva Conventions and the Additional Protocols, looked forward to this, I'm sure, with some trepidation because unlike the ICRC, the United States actually engages in armed conflict. And therefore, what is says—what *it* believes the law to be—what it says the law is—is more significant—with all due respect, Harvey, to your native land—Canada . . . or any of the other countries that pontificate on this subject.

Secondly, it's more of a treatise, exactly in the way that Matt outlined in that it's a resource for lawyers, but that doesn't mean that every word has to be taken as cast in stone and we can already see, thanks to Tom, issues arising with respect to the treatment of journalists from the mere term of "unprivileged belligerent." The way it is used in the Manual reflects, I believe, DOD policy rather than law. It is important because the DOD is really important, and what it says governs the DOD until a higher authority says [something else}. To my simple way of thinking, an unprivileged belligerent is a fighter who is not a combatant and therefore not

entitled to the protections of the laws of war. And not entitled to prisoner of war status if captured. [Such a person, of course, is] entitled to humane treatment, but not entitled to prisoner of war status. And the Geneva Conventions lay out in great detail how you have to treat prisoners of war. So, it's an important point.

When I say it's more of a treatise, I'd like just to focus on three areas. First, use of the term feasibility, which appears in the Additional Protocols of 1977, and the Manual quite properly says a "rule of reason" has to apply to when something is said to be feasible. For example, warning a civilian population that a military operation is going to take place in the neighborhood and that might threaten to inflict harm on the civilians. The Israelis use broadcasts, they use telephones, they knock—that is to say, they'll drop dud bombs on the roofs of buildings as a signal to any civilians to get out of there. In connection with the Gaza campaign of a few years ago, Richard Goldstone concluded that that did not meet the legal standard of feasibility that is required by—that he regarded as customary law. This Manual takes a different view and quite properly so.

Secondly, I would say that its treatment of proportionality particularly with respect to law governing the decision to use force to begin with, I would argue is not correct. It, in my view should be, "that minimal amount of force required to achieve a lawful objective of the use of force." [It therefore is] not, as the Manual says, tied to civilian collateral damage.

Finally, I would say that it adopts a view of the law of war, which I think is a bit expansive to include the *jus ad bellum* as opposed to just the *jus en bello*, the Latin term for the law of war. And *jus ad bellum* governs the law governing the decision to go to war—it's a different animal. And the law of war was designed to ameliorate the calamities brought on incident to war not to protect civilians as this Manual says.

There are other issues that I could get into. My time is almost up—treatment of nuclear weapons, a lot of legal scholars like to say that the law of armed conflict, the law of war, has to apply to the use of nuclear weapons but lets face it people, nuclear weapons are *per se* indiscriminate weapons. A 20-kiloton bomb, that is what was used on Hiroshima, would today be a small weapon. No one

knows quite how tactical nuclear weapons would work, artillery shells and the like, and whether if you were a victim of such attack, you'd actually know whether you were under strategic attack or not and it's just better, in my view, not go down that path. But I've written an article on it, which is just coming out.

I think that, again, [the Manual is an extremely] important document. It's a very good document in a lot of ways, but . . . I think the next step would be for all the service JAGS to . . . develop manuals that are usable and carry-around-able in your kit bag and not just have this as a sort of library of international law for lawyers to use because I think the operational people in the field need to know enough about the law themselves to stay out of trouble. [P]eople in uniform in particular run individual criminal liability for their use of force, their conduct in military operations. It's one of the reasons the United States has so many lawyers trotting around with its soldiers because it was the response deemed appropriate to events like the Mai Lai Massacres during the Vietnam War. So, let me stop there because there's a lot more that can be said but I just want to reiterate that in the main, this a really important document, it's a really well done document, and I, for one, am very pleased that it is out. Thank you.

MR. RISHIKOF: Ok, so Matt, as you, I think, anticipated, the conversation when you produce a document like this generates an unbelievable amount of discussion and contention. The document does [what it very clearly sets out to do], what the major principles are—military necessity, humanity, proportionality, [and] distinction . . . . And then, once those are the governing principles for the entire document, you have the questions that the panelists are focused on.

So I'll let you speak, but there are two things. One is that 'war' is sometimes used as a legal concept, as you put it in the opening of the paragraph. The application or operation of a legal rule may depend on the existence of "a war, an armed conflict, or hostilities. As a legal concept, war has traditionally been viewed as a condition in which a State is prosecuting its rights by military force, usually against another State. However, the precise definition of war often depends on the specific legal context in which it's used." And I

think both of the other panelists have raised that issue of what the context is of the functionality of reporting, or the context of the functionality that Nick has raised, how it understands proportionality and the role of civilians. So, I think we thought it would go this way. So, why don't you take a [minute] and sort of reflect on the comments and those issues."

MR. MCCORMACK: Sure, and maybe the way I'll begin is I'll take [Harvey's] first comment and then Tom's, and then some of Nick's.

You know, on the issue of "what is war?", one of the hardest chapters to write, really [was] the first chapter and the third chapter, which are very theoretical, but they're kind of foundational in many ways. So it's not just a matter of reciting treaty rules and statements that have previously been made in, you know, an ICJ brief the United States has made before the International Court of Justice [or other place]. But, "What is war?" War is not really defined by the Law of War. So this is often an issue of, sometimes in domestic law . . . you may have certain higher punishments for offenses conducted during war. You may have questions of when does the law of war apply in international matters, those *in bello* rules, the rules applied to the conduct of hostilities. So, this is kind of an interesting question that we had to deal with in kind of framing the Manual.

And maybe to pivot to some of Mr. Bowman's comments about the journalist section of the Manual . . . . Maybe first and foremost, I'd like to just make the point that . . . please don't take what I say as kind of push back on Tom, or NPR, or the idea of expressing concerns is somehow wrong or inappropriate, or that I'm defensive in some way. What I would like to do is to push back though because I think the issue of journalists can provide a good vignette to help better understand what the Manual is. And, that's not to say that we won't update and improve the Manual going forward, including the section on journalists. In fact, that's something that we've committed to do. So please take with a grain of salt what I'm about to say.

So first, I totally agree with Mr. Bowman about the difficulty that journalists have on the battlefield. It's an incredibly dangerous

place for anybody – soldiers, sailors, Marines, journalists, humanitarian actors – it's an incredibly trying environment. So, we in DOD—again, I'm not speaking for DOD—but we certainly know that there are difficulties with reporting. DOD policy is to support that reporting.

I mean, this is one of the issues with the Manual itself. The Manual is really about what are the international prohibitions and restrictions. It's not really about how NPR on the ground in Kandahar, or wherever, is really interacting with public affairs officers in the military. DOD policy is that independent reporting is the way Congress, the American public, and other soldiers are to get news about what their military is doing. So, at least DOD policy . . . is very, very supportive of news organizations getting the story, to be able to report on U.S. military activities. Maybe the common example that people like to think of is the idea of embedded reporters, particularly during the invasion of Iraq. I think there were something like 600 [or] 700 embedded reporters that went with units. And, policy is that they are to go with all major units that are available. So DOD, in policy, has been very supportive of the idea of a journalists reporting on U.S. military activities.

And I think [that] with the Manual itself, and the law itself, we have a lot of similarities between the views of DOD and those that Tom expressed. The idea of helping to protect journalists on the battlefield, I believe that's something that's reflected in the Manual.

I'll go into that a little bit more. The idea of avoiding journalists being mistaken for spies is another thing that's in the Manual that we're trying to communicate, that we believe would be in harmony with the ideals of the media and NPR and other news organizations. So, I think we have a lot of similarities there. And we have been talking to news media and journalists since the publication of the Manual in a very fulsome way. We've answered numerous queries from reporters who are writing stories, and we try to help them make their stories as accurate as possible. This is obviously a time-consuming process, but one that we believe is worthwhile. We've received letters, as Tom mentioned, from NPR . . . a very thoughtful letter. I believe that NPR received a very thoughtful substantive letter back. If you've ever received back a note from the

U.S. Government, a lot of times it's like "Hey, thanks for your interest in national security. I've been asked by the Secretary to respond on his behalf," and that's really it. *[with exaggeration]*

What we've tried to do is address the concerns that NPR has raised in a substantive way, better explaining the Manual to avoid confusion, and to actually identify where there are tensions or disagreements. We've done the same with the Committee to Protect Journalists, and other news organizations. My boss has appeared on *On the Media*, which is an NPR news program about media issues. So, we're doing this. And, we'd be happy to sit down with Gary Solis and talk about the Manual, talk about issues. Sometimes the best you can do is agree to disagree, or maybe you find out there's no disagreement.

Maybe I'll just address two things that Mr. Bowman brought up as it relates to the Manual substantively, and I'll try to explain what the Manual is doing and not doing. Mr. Bowman said that we've called him an unprivileged belligerent, or something to that effect. That is not the case. The Manual is not calling journalists unprivileged belligerents. All the Manual is doing is making the point . . . this is the first line of the journalist section: "In general, journalists are civilians." It also says that "journalism is a civilian activity." But, it notes that just like any other civilian, civilian journalists can lose their protected status. They can either engage in hostilities, and it cross-references the section on "directly participating in hostilities," where civilians can lose their protections.

The other kind of unique thing with journalists that we believe is kind of an important point to make, is that the Law of War doesn't control who calls themselves a journalist. The Law of War can tell you what is "direct participation in hostilities;" it can tell you who a "combatant" is; it can tell you who a "civilian" is, who a "protected person" is under the Fourth Convention. But the box of "journalist" is just not defined. So, what that means is that those civilians who are journalists can move to different categories if they do different things, such as spying, or those things.

All the Manual is doing there is making the point that there are ways the Law of War has recognized to help people avoid being mistaken as spies. As the NPR letter to the DOD reflected, there's a

lot of factual similarities. Both a spy and a journalist are collecting information. They're collecting information in the zone of battle. They're doing it to pass it on to someone else. There's a lot of factual similarities.

What the DOD Manual is trying to do is show the legal difference. That is, the Hague Convention of 1907 has a specific definition of what spying is, and we're trying to say, there are ways that journalists can take to avoid being mistaken for that activity, those being, embedding with a military unit, that helps verify who you are and why you're there, rather than just someone random on the battlefield. The other idea is reflected in the Third Geneva Convention: the idea of identification. That helps distinguish who's on the battlefield and why. And this is like a fundamental Law of War principle, the principle of distinction.

So, the Manual doesn't say anybody needs to get an identification document, except that the State has a responsibility in international armed conflict [to issue identification] so that war correspondents can be treated as POWs. But in the case that Tom's talking about in Afghanistan or whatever, there's just no requirement. You don't have to do that. But the Manual is just discussing ways that a journalist can better identify themselves as a journalist rather than being suspicious, or because their activities look similar to spying. So maybe I'll leave it at that.

MR. RISHIKOF: I'll add one more thing, which is quite fascinating. I'll let Tom respond… But just to give you the complexity of the context, the Manual does cite to a UN report in the International Criminal Tribunal for the Former Yugoslavia, where it says, "Whether the media constitutes a legitimate target is a debatable issue. If the media is used to incite crimes as in Rwanda, then it is a legitimate target. If it is merely disseminating propaganda and generating support for warfare, it is not a legitimate target." So that contextual issue is actually quite fascinating as to what puts you over the line of "you are a legitimate target" vs. "you're not," depending on what you're doing in that war effort, either domestic or internationally. I'm sure, Tom, you have thoughts about that.

MR. BOWMAN: The question I have it still the issue of "unprivileged belligerent." As my friend Gary Solis said, going back to the antecedents 1914, it was always understood that an unprivileged belligerent is a civilian who takes up arms. So why has that been expanded to include spying, which is, you know, a vague term . . . sensitive information, as I was saying earlier. What is sensitive information? If I report on how a Marine dies in Helmand, the casualty rate of the Afghan forces . . . They don't want that information out, because they don't want to tell the Taliban. So is that sensitive, and could I be, you know, brought up on charges, handcuffed, dragged out of Afghanistan because of that sensitive information?

DR. ROSTOW: Well, I would raise the question, is it the Taliban they're worried about, or the American people?

MR. BOWMAN: They say the Taliban.

DR. ROSTOW: Because the Department of Defense has a long history with the media, none of which is particularly happy….

MR. BOWMAN: Tell me about it.

DR. ROSTOW: … going back to the Vietnam War. And the whole notion of embedding reporters gives the DOD control. Is that consistent with the First Amendment? Is any of this consistent with the First Amendment? Is any of this consistent with the law of armed conflict, or is it DOD policy that we're reading about?

MR. RISHIKOF: Well, Nick, as you know this is always the *lex specialis*, the idea of war, but the Manual . . . is quite interesting [in] those grey areas. It says, for instance, "Journalism does not constitute taking a direct part in hostilities." Such a person would be

deprived of protection, right? From being made the object of attack. The Manual adds, "In some cases, the relaying of information, such as providing information [for immediate use in] combat operations would constitute taking direct part in hostilities." So again, it's that grey area. I think Tom is legitimately nervous about who defines that grey area, and who has the ability to make that distinction at that moment, and how that will happen operationally while they're on the ground is probably the concern, and I don't know what the easy answer to that is.

MR. MCCORMACK: A lot of issues have been raised. Let me try to address them in somewhat of a logical order. Sorry, I forgot the last point that you made. Oh, yeah, "DPH."

MR. RISHIKOF: It's a DPH, right? Because it depends on the information being provided. And some journalists have gotten into problems in that area, when they've been embedded, giving reports which appear to be helping give positions away and things of that nature. We've had instances of that.

MR. MCCORMACK: So, on that specific issue, what the Manual does is [that] it says exactly what Mr. Rishikof says, and then it cross-references the nine or ten pages or so that discusses what is "direct participation in hostilities." In there, it uses those same words, "passing information on the battlefield," but the examples of that… right… it's just saying generally, this is what it is. But then, the specific examples are very clear, at least in my mind. It's like, acting as like an artillery spotter, acting as like a lookout for combatants.

It's not the idea that a reporter is reporting on top of a hilltop as part of an embed and is working within the ground rules, and is doing exactly what they're designed to do. It's the idea [that] a journalist could, we're not saying that they are, it's not a matter of probability, it's just the idea that, like, a person could lose their certain privileges not to be made the object of an attack if they abandon their neutral role. And just like Gary Solis says, it's the idea

of taking up arms with the enemy. We're not saying that any [particular] journalist is doing that. It's just noting that there is this legal change that can occur based upon people's actions. And maybe, as far as like on the ground, how does this work? This is like a really fascinating thing as a lawyer who has also been a Marine. Lawyers love talking about the law, and these kind of big things about how the law works. But, how things work in the real world are often very, very, very different. For instance, the rules of engagement that those forces are working under, their particular mission, and all those types of things naturally and responsively hem in what happens in the real world. So, . . . these legal big [issues] are something different from what's on the ground. So, for instance, the rules of engagement or the specific mission that a unit is on is going to drive things much more than these issues of international law and what's prohibited and what's restricted.

And then . . . maybe just on the last piece about sensitive information, because we've heard this several times . . . the issue in that section really isn't, like, running afoul of passing sensitive information. Really, it's just noting that States have found a need to restrict [the] passing of information during wartime. And, this is not a terribly unique thing. Like, so, for example, I don't know if Tom's ever been an embed…

MR. BOWMAN: Yes, many times.

MR. MCCORMACK: So there's like ground rules, right? Where you agree to certain restrictions?

MR. BOWMAN: Right. And the big thing is operational details. And my people at NPR, and the Committee to Protect Journalists, everyone agrees that you never say, "Next week, they're going to go to Helmand province, to Lashkar Gah, and mount this serious big operation. And I've been told many times information about operational details, and the Marines always knew I wouldn't tell anyone. And I said "How do you know I'm not going to tell anyone?" They said, "Because you're coming with us!"

DR. ROSTOW: "And we have the guns, and you don't!"

MR. BOWMAN: But clearly, issues like that, again, you would never reveal that, because you don't want to get anyone killed. How could you justify that? But again, these sweeping "sensitive information" make me kind of nervous. Because in this day and age, with this particular administration, this particular Pentagon, everything seems to be sensitive. That's what I worry about, that I've seen.

DR. ROSTOW: One of the things that I think is really good about this Manual is that it has a running commentary on the Additional Protocols of 1977, and on certain interpretations of the law of armed conflict and the applicability in armed conflict of international human rights law, because there is more than a hidden agenda among some advocates of certain interpretations of the laws of war, that the laws of war should make wars unfightable and illegal. That is not the purpose of the laws of war. The purpose of the laws of war is to ameliorate the calamities that are an inevitable consequence of warfare. And I just wanted to make that point, because I think it's an important one.

[AUDIENCE MEMBER]: And so what I'd ask you, Sir, Mr. McCormack, is you know, you said you had this vision for the Manual. Well, you know, visions, much like hope, is not a strategy. So if you could, Sir, my first question would simply be, I'd love to hear your plan to kind of spread this gospel throughout the DOD, in particular throughout the JAG Corps, perhaps to commanding officers, along those lines.

My second question, Sir, actually pertains to the Army. They had some verbiage in their manual. The language was essentially that the citizens of one nation are at war with every citizen of the other nation in a period of declared war. That language was not brought forward into this Manual at all. It's mentioned in a footnote, but it's

not really addressed. I don't know if you know even the details of that, but I'd love to hear why that was not adopted in the current Manual.

MR. MCCORMACK: So, the vision that I talked about was how the Manual will be used. We have put it out there. It's online. I think it's a marketplace of ideas, in many ways. Smart judge advocates, and the military schools that teach new lawyers and teach continuing education, that teach international law, are going to be using it. And, I've seen it used more and more, even though it's only been out several months, in operational [settings] and other reasons as people are thinking about what are the rules expressed in the Manual, the rationale for them, whether they apply in a specific circumstance, [and] what are the other policy considerations to take into account.

So, I can't say we're going to spread a gospel, in a way, but I think the strength of the Manual is its value to practitioners. If they find it valuable, they're going to use it, and they're going to use it more and more as they realize its value. Like I said, I literally use it every day, just because I find it super valuable. I think judge advocates who are really practicing the law of war will do the same. It'll be, like, how did I ever do this before I had this Manual?

Granted, it is different than the 1956 [manual on] Law of Land Warfare. It is not 123 pages. I love that document. It is a beautiful thing of simplicity. The problem, in my view, is you can't have that same Manual today. There are just more legal issues, more treaties.

And then the other thing we wanted to do [in the Manual] . . . you'll notice there's copious footnoting. That footnoting is for a purpose other than just to footnote. What we really wanted to do is provide transparency in the Manual. When something is in the text, we want you to know why we're saying it. We want to remember why we said it in the first place. So the footnotes are really the rationale for the main text, and it tells you the weight of the reason why the information is in the main text. Is this coming from a treaty? What is the actual treaty language? Is this a U.S.

interpretation? Is this a DOD view? Is it unfootnoted? All those things matter to transparency in legal discourse.

On the issue that you mentioned about the previous manual, noting that persons of an enemy state in international conflict are the enemy. In a way, I think that's probably what it says or something similar to that. Like you said, I don't think it's in the main text, but the idea's still in there.

This idea, it's like so much with the law of war. That is true in so many ways, but it's untrue in so many ways. Because we think of different rules as they relate to… the proportionality rule for attacks and whether the anticipated collateral damage would be excessive to the military advantage expected to be gained. So many people think about the law of war in terms of civilian protection, although the law of war is also protecting combatants, right? Those balances found in the law are a balance between the ability of people to protect themselves in a war and the ability for people to be protected in a war. So there's a fine balance going on, I don't think it's included, I can't say why it's not in the main text, but it could be very confusing to people, because they [could] think that you're [mistakenly saying that] all civilians of the enemy State [are] targetable. [Even] if they're a journalist, they may be made the object of an attack. People can easily misconstrue that, if it's not well-explained why you're including it. So, it may not have been worthwhile to bring that issue forward [in the Manual's main text].

MR. RISHIKOF: Well on that issue . . . One of the more interesting things that's happened in the past week is the attack in Paris, and the fact that the President of France has said "We're going to declare war on ISIS." And from a law of war legal doctrine, the United States was I think the first nation in the authorization of the use of military force [in 2001], which declared war not only on States, but organizations and individuals. So, we have helped create contextually, this new ability to project force, military force, against particular significant organizations.

[AUDIENCE MEMBER]: The "s" in "ISIS" stands for "State."

MR. RISHIKOF: Well, the interesting question also is whether it's "IS" or… it's different variations, right?

[AUDIENCE MEMBER]: Even if it's "IS", the "s" stands for "State."

MR. RISHIKOF: So, this is one theoretician that says this is an easy one, because of a geographical [territory]… But we are not signatories to AP I, and that's one of the interesting questions of whether or not the law of war applies when you're in a NIAC or IAC, and how you define a NIAC . . . non-international armed conflict and an international armed conflict . . . So it's one of those issues I think this Manual will be used… Yes, Nick.

DR. ROSTOW: One point to remember is that President Lincoln issued the Lieber Code, [General Order 100], as Matt said, but he never regarded the Confederacy as a State, he regarded it as rebels, but nonetheless, treated captives as prisoners of war, and conducted blockades and so forth and so on. But, it was a nice distinction that may not have made a difference.

MR. RISHIKOF: Well, it's an interesting question as to how one defines State and who gets to define what a State is.

More questions.

[AUDIENCE MEMBER]: I'm wondering how much influence you foresee this Manual will have on combatant commanders when developing ROEs and command directives.

MR. MCCORMACK: I don't think it's going to have a lot of influence on that, and this is the reason why I say that. Rules of

engagement are a combination of factors… there's various considerations. Some of them are operational, some of them are legal… there's lots of different reasons. But the law of war is like the outer limit of what may be done, what international law would otherwise prohibit or restrict.

The state of the law was the same before the Manual was published as it is afterwards. So, that's not going to change the outer limit. And then also the operational design of the commander that's going to work within that framework, really isn't going to be influenced by the Manual, because the Manual really isn't telling [him or her] how to conduct the operation. That operational design of how to defeat the enemy or to impede its progress or to interdict its movement is really going to be something that's part of the operational art that they're doing today, and I don't see the Law of War Manual really changing how they want to advance a military objective as it relates to designing ROE.

MR. RISHIKOF: I remember when I used to teach at the National War College, we used to have a slide of what the rules of engagement were, loosely, in World War II, versus the rules of engagement in Vietnam. And the Vietnam slide went on for a number of slides about how force could have been used in that particular conflict. As Matt is saying, the politics of the matter became very powerful in influencing how we understand the rules of engagement.

Any more questions?

[AUDIENCE MEMBER]: I'm Jeremy Rabkin. I have two questions, one for Mr. McCormack and one for anyone on the panel. The first is, could you just tell us a little more about why this took so long? There were some complaints, sort of a suggestion that the Obama Administration was sitting on this, holding it back… maybe you could tell us more about the history. And then, I'd like to hear more about, if I could say, the philosophy of this. If you put out a thousand pages, it suggests, there's really a lot of law, a lot a lot a lot

of law. And even if you say, no, don't worry, it's only online, we're revising it all the time, that doesn't make it less law.

So, was there concern, and do the rest of the panelists think maybe there should have been concern, if there wasn't? That this is contributing to the over-legalization of military activity and maybe this was wiser in the 1950s when they said, eh, a hundred pages, that'll do it, there are just a few rules, after that you're on your own. Is it really progress for us to try to go into such detail, and have the internal revenue code of armed conflict?

MR. MCCORMACK: Thank you for your question.

MR. RISHIKOF: I think he meant the analogy to the IRS in a positive way!

[AUDIENCE LAUGHTER]

MR. MCCORMACK: So, why did it take so long, or what's some of the history? Maybe the best way is I'll summarize some of the history, and then maybe I'll see what else I can address.

So this Manual had been in the works for a long time, that's the bottom line. When we look back, we see memoranda from the 1970s, where the idea would be that there would be an all-Services manual that would be kind of DOD sponsored. And a lot of this was developed out of the idea that we would ratify the [1977] Additional Protocols [to the Geneva Conventions of 1949], because obviously the United States participated in those multilateral negotiations, and there was a question as to whether we would ratify them or not. And if we did, we would certainly need to update our legal guidance to the field, through, like, a new manual. This idea kind of continued to percolate.

We never did ratify the Additional Protocols. That's, like, a good reason to delay a project: "Hey, we may do it tomorrow, we may do it tomorrow." But then the decision was made in the late 80s

not to [ratify Additional Protocol I]. But then its like, okay, that decision's been made, at least for Additional Protocol I. Additional Protocol II, which applies to "high-intensity NIAC" for a lack of a better way to express it, is with the Senate awaiting advice and consent. But the idea of updating the law of war manual based upon whether we were going to ratify AP I was resolved in the late 1980s. Like any project within the government, unless someone is asking for it, demanding it, things always take a higher priority. That's my only guess.

I know I work in a bureaucracy, as Mr. Rishikof said, when Stephen Preston, the former DOD General Counsel, said "This is one of my three priorities, it's going to get done," what do you think happened? It got done. So it's a matter of prioritization within a large organization. I don't know, I can't really assign or try to guess people's motives, or reasons why it took longer. I think probably 9/11 probably had people focused . . . a good portion of the legal community . . . so, that's also probably not a contributing factor to getting it done. But, I can say when Mr. Preston got there got there, it was probably 2012 or so, it was full steam ahead. I know that there's been suggestions that the project to write the Manual had collapsed because of political influence or interference, but that's not my experience. It's as simple as that.

DR. ROSTOW: Have we over-legalized the law of war, or warfare? I think every time the United States has been in armed conflict since World War II, and probably during World War II, the people in uniform, the people responsible for directing military operations, have been accused of war crimes. This was certainly true in Korea and in Vietnam.

So, that heightens the importance, if you will, of the laws of war, of conducting military operations in a manner consistent with the laws of war. Usually people who say that "so-and-so's a war criminal" don't know the laws of war, and really are making a political rather than a legal statement. But it's the kind of thing that carries with it real individual liability. Officials of the George W. Bush administration do not travel to certain places because of fear of arrest. So that's one thing.

Secondly, there have been a lot of conflicts since 1945, or 1949, when the Geneva Conventions were adopted. And, if you think of armed conflicts kind of like courts, that's where the law of war gets applied, gets amplified, [and] decisions get made as to what things mean and how to understand them. So, there's accretion to the law of war beyond what is written in the text. It's interstitial, if you will, to use the term Justice Cardozo used so famously. It's the way law grows.

Is a thousand pages a lot? It's a lot, but there are a lot of treaties, there's a lot of custom, and interpretation. Now, this is the Department of Defense view of what the law is, and what US policy in the field is, and that's enormously significant, and will have enormous impact, I hope positive impact, on other countries and the way their military is trained, their lawyers are trained, and what they think the law is. It might even have an impact on the International Committee of the Red Cross. That would be a useful thing. It might even have an impact on the International Criminal Court. That [also] would be a good thing. So, it's a hugely important event, and I think [that when] the Obama Administration [is] long forgotten, this Manual will still be used and looked to. So . . . Matt, you and your team have achieved immortality.

[AUDIENCE LAUGHTER]

MR. BOWMAN: From my perspective as a reporter, I'm always troubled when I see more rules and regulations. As it stands now, I have to fill out so many forms to embed with American troops its like buying another house. And they ask what stories you're going to be working on, and it's just troubling, and when you look at the issues of unprivileged belligerents and sensitive information and all this stuff . . . Neil Sheehan, who of course covered Vietnam, just did a piece for the New York Times. He found some pictures of the Ia Drang Valley fight in '65. We just passed the 50th anniversary of the first big battle in Vietnam. And, he talked about how back then, you could just hop in a helicopter and go out with U.S. troops. You didn't have to sign any damn papers, or your signature or blood type, or are you going to have a heart attack, or do you take any

medications. You would just get on the god-damn bird and go. And, it all worked out well.

[AUDIENCE MEMBER]: Except for the Vietnam part.

MR. BOWMAN: That part, yeah.

DR. ROSTOW: And journalists who got killed. I mean, he didn't get killed.

MR. BOWMAN: We lost a lot of friends and colleagues in these wars. And, I remember right before the Iraq war started, we went down to Fort Benning. They put a lot of the reporters through training to see how you move with soldiers and all. They mostly did it to make fun of us, to see what we could do, and how quickly we could run, and all that other stuff. But, Hal Moore was there, and he talked about reporters and what we do. He said, "Anytime I went anywhere in Vietnam, I always brought reporters with me." He said, "The American people have a right to know what their sons are doing in their name." Particularly something like this. And, I think we've lost that.

Nothing against the Manual, but all these terms that we're bandying about . . . I mean, come on. People don't like reporters, but we're not spies. We're not going to pick up a weapon and fight anybody. I mean, this is ludicrous, some of this. And again, filling out these rules and regulations, and abiding by all this stuff… You know, you can't take pictures of the dead… We'll, how are people going to know what happens in war, if you have all these rules and regulations?

My neighbor's a guy named Norm Hatch, and most people don't even know his name. He was a Marine combat cameraman in World War II. Landed at Tarawa, walked in 300 yards, because they messed up the tides, held his camera over his head, saw people die to the left and right of him, got to the beaches, never got a scratch. So,

he takes all these videos and pictures, dead Marines floating in the water. First time anyone had taken pictures of dead Americans in World War II. He was a Marine, so they roll up all this footage and send it back to the West Coast. The Marines look at it and say, "No way anyone is ever going to see this." But, the Marines worked it up… others, I think, worked it up, and it got to the White House. It got to Roosevelt. And Roosevelt called in Robert Gerad, who some may remember as a great Time magazine reporter. This would never happen today. The President calling in a reporter and saying "Hey, what do you think about this stuff?" And he said what Hal Moore said. "People have a right to know what their sons are doing in their name."

MR. BOWMAN: Roosevelt said ok, run it. Ran on newsreels, all that stuff you would never see today.

DR. ROSTOW: And there was no censorship during the civil war.

MR. BOWMAN: Right. So it ran on newsreels all across the country in movie theaters and went on to win an Academy Award. Never happen today. Never. It's kind of different from what we're talking about, but it's part of the same issue of rules and regulations and we're going to sanitize it, you know H.W. Bush saying were not going to take any picture of caskets, flag draped caskets, coming out of Dover. You know, this is, I'm sorry Matt you're a good guy but this is just one more instance of censorship, and let's not tell people what's really going on. Sensitive information, unprivileged belligerent, it's one more evidence of that. I really think it is, and everybody here should think long and hard about that. You know, how many people here have, you know I can see some Marines here, but how many people have friends and neighbors, or know people, family members doing this kind of stuff? No one! Most people don't, less than one percent. It's easy to sanitize it. And it's wrong.

MR. RISHIKOF: I would say, what's interesting Tom, is that there is a distinction between the policies of an administration, deciding how war should be reported, and the Manual which is trying to lay out the rules and [regulations] about how to project force, of which a small section is, the reporter section. And, the pieces I read demonstrate . . . the distinctions and problems that they're having in modern warfare. I see it more in that kind of, that's how I see the distinction. Let me give you an opportunity.

MR. MCCORMACK: Thanks. So maybe just briefly on the issue of taking pictures of dead bodies, so obviously there is a bit of a tension, right? The desire to inform the public, but, and although the law of war doesn't say how reporters should report things, there are protections for the dead within the law of war itself—a certain respect for them and other issues that any policy would have to be consistent with. I'm not saying that the policies that you were dealing with were or weren't, but it's the idea of taking pictures of dead bodies could be contrary to some of these principles that are protected in [the] law of war.

I forgot to mention the issue on the voluminous nature of law of war. So, maybe I'll talk about the Manual itself and then about the law or war writ large. The idea when we were writing the Manual [was whether] you could make it shorter, right? You could make it shorter by summarizing the law, or you could make it shorter by leaving things out. We didn't want to summarize the law because we thought legal practitioners really wanted to know what the treaty language was, or what the language that was used in the statement that would assert what the interpretation of a legal rule would be. If you summarized that [information, the Manual] has so much less value [to the practitioner] because now [he or she has] got to look up the thing in the original document. So, [the Manual is] lengthy in the way, in some ways because we wanted to be really helpful to a practicing lawyer.

And, then the other issue is, you could have left stuff out, right? The easiest thing is, the [example of] Swiss francs. Why would you mention Swiss francs for POWs? Well, when you're looking at [the Manual], it's online. It doesn't matter that there's a section on

Swiss francs, unless you need to find something on the Swiss francs rules, right? Because on the computer, it's just a screen, right?

And so, the idea of completeness was important to us because there may be somebody who has to figure out whether we need to provide a canteen for the POWs, [or whether] we actually have to pay [POWs], right? The Third Geneva Convention requires advances of pay; this is a treaty obligation. Somebody may need to know that one day. And, then we were also informed by the idea that humans have this innate nature to [assume falsely] that they know what the future holds. We will never do an occupation again, you know? *[rhetorically]* We will never have to conduct another amphibious landing, you know? *[rhetorically]* The evidence of that was countered, you know, in the Korean War, right?

So, we just realized that it's impossible to just strip things out under the guise, or under the thought, of "oh, no one's ever going to need this." And, so we erred on the side of completeness.

That said, I do have real concerns about the voluminous nature of legal rules as it relates to armed conflict. And, it's not because of the rules themselves, but because the law has to be extremely intuitive and normative to people who've never opened up the Geneva Conventions and read them. It has to be innate; it has to be understood. You can do a lot of that in training and discipline, but [problems arise] when rules become exceedingly complex [and] when they're applied towards more tactical operations, [rather] than places where you have more time to deliberate [and where] you can get a lawyer or two there to help sort things out.

The real danger you have with the law of war not really making sense where it matters most, which is on the battlefield. The real strength of the law of war isn't so much in its legal nature and effect *per se*. Sure it has strength because, as Dr. Rostow said, you can go to jail, right? That has an effect. But, really the power [of ensuring compliance] on the battlefield, in my mind, is the fact that [the law] should embody shared values that are embraced by military professionals. They're going to [comply with the law] as a matter of course, and so the complexity [in the law] makes [implementation] much more difficult.

[AUDIENCE MEMBER]: It has to adaptable; maybe that's a combination of perception the more voluminous it is, the more you discourage the notion that this is the general rule. Of course it would be adaptive. That seems to me the danger of [inaudible].

MR. RISHIKOF: Right, so this is always the tension between the common law and the more famous continental law, and statutory law…

[AUDIENCE MEMBER]: And common law countries.

DR. ROSTOW: But, also it's a tension embedded in such things as the ethics laws that govern federal employees, which ought to reflect common senses about what's ethical behavior and what isn't. But, anything but, it' as complicated in its own little way as the Internal Revenue Code and you can act ethically and violate it.

MR. RISHIKOF: Let me make more of a different type of point here, which is that: So the first is, one of the segues we have for the panel was to talk about the cyber issues. So, when you turn to page 994, it's about 15 pages, which is very elegant. But it says, it begins for most of the law students like the beginning of a Bluebook exam. It says precisely how the law of war applies to cyber operations is not well settled, and aspects of the law in this area are likely to be continuing to develop, especially as new cyber capabilities are developed and States determine their views and response to such developments.

So, it takes, so we know there's the Tallinn manual, the Tallinn Manual is out, [and it is an academic study on how international law applies to cyber conflicts]. There's going to be Tallinn II coming out, to deal with that classic question of "When does cyber issues rise to the projection of force is below the [threshold and is] just a criminal matter."

So, you guys I think were helpful in saying "here's sort of where we're at." So, one of the advantages of the Manual is that it identifies ranges of issues that require more study, and will help focus discussions. So, I use it to help focus discussions and walk through the cyber operations to figure out what are the issues we know, what we don't know.

The second issue, the length of it is, this is a little bit different because this Manual, [which] is a Manual that is used in order for us to [lawfully] kill people. Because that's what we do at war, we kill people. So, you really want a certain level, clear justification, black and white, as to what's appropriate or inappropriate. I think the soldiers on the field deserve that from their [lawyers and] commanders. And, it's a little bit more detailed than other types of law.

The example I'll give you is, so there's probably going to be an issue about whether or not the President has the authority to move prisoners from Guantanamo [Bay] to CONUS [the United States]. And, there are two [sections involved]. The Constitution is very short, it's very clean, very adaptable; Article II power appears to give the President that power and Section 8 very clearly says that Congress has the power to declare war, grant letters of mark and reprisal, and quote make rules concerning captures on land and water. There seems to be quite a clear black-letter Constitutional law, but yet there's still dispute and I think that's sort of an interesting phenomenon that [still] two hundred-plus years into the republic, that particular power is not clear as a Constitutional matter. I may have one view, but another Constitutional lawyer may have a different view about where the power resides. That level of ambiguity at the Constitutional level, [is] interesting; it really defines where we're going to see the power.

But at the level of "can you define this person as a combatant?" That's a rather important phenomenon for people who are on the field. And so it's quite lengthy. Now, I think your position might be, "Professor, is that 'does it remove the ambiguity of some of these issues?'" And, there it doesn't, because a lot of it is contextual, but will it in the end provide the rules as to whether or not, as we always say, "are you going to pin a medal on the person, or

are you actually going to have an Article 32 trial against the individual?" And, that's rather important for people who are actually the practitioners.

So an attempt to try to [set the rules] is why people wanted the Manual out, because they really wanted to be able to see where the left and right margins are. You may be dissatisfied, you may not be happy where the margin has been drawn, but it actually helps you to fight back and say "that's the wrong margin, you should push it back." That's actually quite helpful as to where we are in 2015 on these issues. So, that's how I would respond to the length issue too. Jeremy, you may not like that, but it's a very credible response, really. As a Professor, it's definitely an A-plus response.

Sir, why don't you identify who you are and wait for the microphone, sir. We just need it for the record, because we want to memorialize your thoughts.

[AUDIENCE MEMBER]: You don't!

[AUDIENCE LAUGHTER]

Two questions, or one question and a comment.

Are there any sections or chapters that are more important than others, that inform the other chapters so that you can get into it easier than just reading from page one to page, you know, twelve hundred?

Secondly, it seems to me that, I mean there are so many uncertainties, and a law of war. I mean it's almost an oxymoron, just a law of war. You're talking about chaos; when you really need this Manual, you're really talking about chaos, and there's so many levels of understanding, from the snuffy that's the infantry man in the front line, and doesn't know whether to shoot or not, to the commanding general who says "ok we're going to go in there and clear out this mess," and some people might take him literally, and they do clear out a mess. It's sort of like, you know to me, it's sort of like if we had

marksmen over here shooting at you with live rounds, ok. But they're marksmen and they're not going to kill you, ok. And you're trying to conduct a discussion about war with that happening. And of course, that's what happens in war, without the certainty that you're not going to be shot. This is, you know, the cloud of war, my lord, it's something real. And maybe what my, what I'm getting to is, the understanding of a Manual like this is going to be different all the way down the ranks.

MR. RISHIKOF: So let me respond, and I'll let the rest of them respond. [W]e always used to bring Father J. Bryan Hehir to the [National] War College. He's one of the most popular lecturers. He's been doing it now [for] almost seventeen years in a row. So Hehir always begins the lecture with "there are no rules in love and war." So, the left margin is there are no rules. The right margin is "I'm a pacifist, I never believe the use of violence is ever justified, therefore I will never fight."

So, those are the parameters of the debate, but we have decided that there actually should be something as collective civilizations; we've agreed, there has to be something about the rules. One of the arguments always goes back to the Lieber Code: Lincoln's goal was to reincorporate the South. So, because he knew the ultimate goal was reincorporation, he felt if they did take a destroy and waste approach to the South, they would never be able to have the South rejoin the Union, because they would've created such animosity and hostility in the way they prosecuted the war, and treated the prisoners, that his ultimate the goal of the Union would've been defeated. So what's very intriguing about all of these [military codes is that] it starts with an internal civil war, it's really a NIAC, not an IAC, an international armed [conflict], but one of the reasons I think we want to do it this way is because in the end, the ultimate goal of war is to have the individuals we are fighting to join the "Borg." We want them to join the world of civilized nations. And, therefore we believe conducting [war] in a certain way allows that argument to be made. That's the position that we think, I think, is why this is very elaborate. It's an extraordinary amount of documentation, how you treat individuals down to prisoners of war,

which is why we had the Red Cross, but it's because in the end, that's the ultimate goal of projecting force. So, that's, I think, the philosophical answer. But I'll let my other colleagues respond.

MR. MCCORMACK: Maybe if, gentleman in the middle, might I go first?

On the issue of like the fog of war and the chaos of war, I think one of the interesting things about the law of war is in many ways it recognizes that. A lot of our treaty obligations were negotiated in the aftermath of World War II, or in the aftermath of Vietnam, where military judgment is incorporated in many ways in the rules themselves.

For instance, the idea of taking feasible precautions—that's like a military judgment of what kind of precautions you are to take before an attack. The idea of not to cause excessive collateral damage, there's flexibility in that rule, right? And it's a rule of military judgment as to what would be excessive in relation to the military advantage to be gained from the attack.

So a lot of these ideas are already incorporated in the law of war, and also reflected in the Manual.

And maybe the last point about this, is another thing that is reflected in the Manual is that the judgment of combatants is judged by what they knew at the time, not some *ex post* analysis, or I guess, yeah, some *ex post* analysis of second-guessing them. Everyone understands that the enemy is trying to deceive you; you don't know what the heck is going on; people are shooting at you; and it is a very difficult environment to do what you want to do. And so, a lot of the law of war already reflects that.

And then maybe, this point about where the heck to begin with [the Manual], right? It's so long. Is one chapter more important than the other? So, [the answer is] "no;" no chapter is more important than the other. That's the simple answer.

But this is what I would do, if I was like in maybe your shoes or anybody in the audience. I would look at the newspaper and, say it's two years ago, I think it's been two years ago, when the Assad

regime, the Syrian regime used chemical weapons against their own people as the allegation goes. I would type into the "find" function "chemical weapons" and I'd say [to myself], "what does the Law of War Manual say about this?" You'll go to a section that's about chemical weapons. You'll read it. Like I said it's chunked down. So, you can say "I'm going to read the three or four sections," or you can say "I'm going to read one [because] I'd rather read the rest of the New York Times or the Washington Post."

But, I would [review the Manual] issue-by-issue as things pique your interest. Because like I said, I wouldn't recommend anybody read [the Manual] from beginning to end, just because it's just too much.

What I do find though is [that] I never know [what] the thing is going to be that I'm going to need [to use the Manual for]. That's why I say no chapter is more important than the next. I'll get an issue and I'll think—like today, I had an issue about when are the end of hostilities? This is an issue as it relates to the detention at Guantanamo, right? I wanted to see what we had in the Manual about that as it relates to the Third Geneva Convention [and] the Fourth Geneva Convention. When I started [my day] today, I didn't know that I would want to know that information, right? But, I looked [and] I found it in three minutes. It's right there, and now I know that issue. It's refreshed in my mind and I can go about my day, or give the advice I need to give. So that's my advice.

MR. BOWMAN: Well I'm not a lawyer so, you are right about the fog of war. War is difficult on lawyers, I think, and soldiers and journalists as well. Particularly insurgencies, how do you tell an insurgency's succeeding? I always tell people if there's one thing harder than fighting an insurgency, it's covering one. But, as far as legal issues, I'll turn it to Dr. Rostow.

DR. ROSTOW: Well, I think that Matt's points were good, and I think Harvey's are too. I would just add that one of the useful objects, I don't know why they put John McCain as a POW on the cover, but if you want to know how to treat POW, and whether

torture is permitted, the Manual will tell you. And, it would've been helpful to have that . . . .

MR. RISHIKOF: You just raised an interesting question, which is, we have *jus in bello* and *jus ad bellum*, [and] some people have talked about *jus post bellum*. *Jus post bellum* is when hostilities end, right, what's the appropriate role? Which is another cool area, potential area, of thinking through rules and regulations. So, if you don't think this is long enough, Jeremy, there's like a whole new volume that could be generated for that. More questions, yes sir?

DR. ROSTOW: Let me just add one more point, which is something that Matt said. It is one thing for the U.S. Government to say . . . what is excessive, what is reasonable, *et cetera*., this commander's judgment about what is reasonable under the circumstances. That's really important to say, and for the U.S, Government to say, for DOD to say, because there are scholars, there are rapporteurs for the United Nations, there are judges in international criminal courts who don't agree with that.

MR. RISHIKOF: He's passing the parole as we say in France. That'll be around later, Judge, if you have a point. Mind saying who you are?

[AUDIENCE MEMBER]: I'm Peter Macchiaroli, I'm a 2L and I'm a candidate member for NSLJ.

You know in the last fifteen years or so we've really seen the rise of the prevalence of use of private military contractors. In Iraq, it was estimated there were over one hundred thousand mercenaries there at one point, and you know we've seen some of the issues that are associated with that. And, so I'm curious if this Manual was all designed with that in mind? Was it intended to clarify or assist them in any way? Does a lot of the material in there cover them, and if not, is that something, do we maybe need a companion or something that would enable, and clarify some of those issues?

MR. RISHIKOF: As you know that was a hot issue—which rules govern contractors?

MR. MCCORMACK: So, the issue of private military contractors isn't really a focus of the Manual itself. That said, the law of war applies regardless of whether you're a contractor, or you're a civilian, or you're a combatant. So, [the relevant rules] really depends on what you're doing, right?

So, it's like, the issue if you're a person accompanying the force, and it's an international armed conflict, that's covered. If you are a person who's a civilian and you're directly participating in hostilities, that's covered. If you are a civilian contractor and you, you [do] any number of things, that's covered.

It's not written from the framework of "Oh, I'm this person. I'm a contractor; here are the rules that apply to me."

Really, the way the Manual is written is from a functional approach. It's not written like "here are the rules for combatants in one box." "Here are the rules for civilians all in one box." "Here are the rules for contractors all in one box."

Really, it's a functional approach, and that's the way the law of war works. Some people explain [the law of war] in these big boxes because it's a very easy way to explain [that] "combatants can do 'x'." "Combatants can't do 'y'." That type of thing.

But really, so all the rules for private military contractors are in there. They're just not framed as for them specifically.

MR. RISHIKOF: But, there was an issue at one point as to whether or not jurisdictionally, they would fall under the Court of Military Appeals or they would fall under [an] Article III court, right?

So if you're looking for interesting law review articles, how the Manual and our statutes have covered that was a bit controversial during the last fifteen years that we've been at war. [Y]ou might

want to look and there's some scholarship on it, but it's an interesting topic about how the law is going to approach that issue. More questions? Sir.

[AUDIENCE MEMBER]: David Hart, retired Army, currently a 1L.

My question goes to the international piece, and really to all the panelists. Have you had any feedback from international organizations or other countries that you can talk about, about this Manual? Do they see their countries or organizations adopting it, using it, doing something similar?

MR. MCCORMACK: So we haven't had a whole lot of international feedback yet.

My boss is actually in Israel right now giving some remarks at a conference of legal scholars. I think that'll pique some people to provide input back to us, which would be very helpful.

The only real thing that I've gotten back from other foreign militaries is they appreciate the way we've documented the Manual. The reasons why we've stated what we've said in the main text by footnoting. [It's] an issue of transparency. It's not helpful to just state a bunch of rules in the main text and not know where the heck they're coming from, or why we're saying it.

If you can look in the footnotes and you can say "Oh, this is a treaty that we're a party to or not a party to, that's why they're saying this rule wouldn't apply to me" or "this is a U.S. interpretation of a legal rule; we may have a different interpretation in Canada or France or something." It allows them to really understand what we're saying and why we're saying it.

And like I said during my initial remarks, this isn't a codification of customary international law, *i.e.*, trying to say "oh these are the rules for everybody," right? It's more about what are the rules for U.S. forces under international law, regardless of their source.

So, that's the one point that I've gotten back is [about our] transparency, rather than a lot of other legal texts that are written vaguely in order to try to advance [a particular point of view as] universal.

MR. RISHIKOF: Though as you said, the first fifty pages are quite fascinating in the Manual, because it does engage the community as to what are core documents, so the relationship between human rights treaties and the law of war. It has a section on different views on applicability of human rights treaties. The International Covenant on Civil and Political Rights, that we're a signatory [to]. So it lays out sort of the framework, which is, not many documents do, and that allows you to engage, I think, as Nick was saying, it very clearly says there is a Convention against Torture.

[AUDIENCE MEMBER]: It sounds like we're not aware of anybody else having done such with the document? International organizations or entity.

MR. RISHIKOF: They are. I think probably the ICRC will be coming out with lots of views. I would say over the next six months to a year, to two years, there's a whole range of organizations that are engaged in this document, to try to respond to it, what they like, what they don't like, and we're going to find it.

MR. MCCORMACK: Yeah, I would expect that too. And, I think this volume gives people some pause and [they need] some time to think about it. The way I would actually really expect to see it used in some way is in the way that we used other military manuals. When we were writing this Manual, we referred to the UK Manual, Canada's Manual, Germany's Manual, and this is something that DOD and the Army before DOD did with the earlier manuals on law of war.

Many times, militaries will look at each other's manuals. What will be interesting to see is if military manuals going forward

look more like the DOD Law of War Manual. Some people may not like that, but it'll be interesting to see its influence on how people design or state their rules, because they may in fact be influenced to [do] that.

MR. RISHIKOF: I know the American Bar Association is going to put together a workshop with our National Security Law Committee and the Military Committee to review the document and do a small, short, white paper on what the issues are that people like or don't like, or considered controversial and may require more work. I know it's hard to imagine, but it's almost 9:00. I mean, the time has flown on this subject.

MR. MCCORMACK: There's my wife yawning back there!

[AUDIENCE LAUGHTER]

MR. RISHIKOF: Well it's funny because I actually gave Mrs. McCormack an opportunity to ask her husband a question in public, if you like?

Is there anything that you'd like to have him say, anything either on the Law of War of any other subject?

DR. ROSTOW: Sorry, Harvey usually embarrasses me with that sort of question, so…

MR. RISHIKOF: So feel free! I'll make sure you've got the last question if you want it. Last question then. Well then I'll give each of the, last question sir?

[AUDIENCE MEMBER]: [inaudible] Crawford, also retired military, Army intelligence. This theme of non-traditional actors in

the contemporary operational environment. Point of question: are cyber perpetrators combatants? And two: are bloggers, posters, and people who tweet, are those journalists in your opinion and deserving of those privileges you spoke of earlier?

MR. RISHIKOF: So Tom maybe you could help the Supreme Court in this area? Define what is a journalist?

MR. BOWMAN: Well, one of the sad problems today is that any person can call himself or herself a journalist. You can be a blogger; you can sit in your mother's basement eating her cookies and can call yourself a journalist. I've talked about this before…

MR. RISHIKOF: A tough issue.

MR. BOWMAN: Yeah right, right! Yeah, we do have cookies here and they're very good!

[AUDIENCE LAUGHTER]

That you know, any person can get out there and call himself or herself a journalist. You have political operatives for certain campaigns, we see now ABC News. I mean that's just a troubling thing I see in this day and age.

But you're right, I mean all these people could end up on the battlefield and who's a journalist and who's not a journalist? It raises other issues for you in tying to work this thing through.

MR. MCCORMACK: And maybe the short answer to your question is "no." The Manual doesn't answer that question. I can't remember exactly what [the question] was but it was very detailed.

Really the cyber [chapter focuses on what] we have said already, and I don't think we've addressed anything [that] specific in a public way.

MR. RISHIKOF: But, we have said that it's clear that you can use Title 18 as a criminal matter, and we've put out indictments of individuals who've used cyber, right?

I think it is envisioned that if there are [differences], we're shrinking the difference between the kinetic world and the cyber world. And, that you can have cyber strikes that have kinetic impacts. And, if that happens, one would think there is, we would call them a carbon unit, is sitting behind that terminal. They might, depending on the context, would be a potentially lawful target, clearly if they're wearing a uniform, and we're in war.

But, the interesting question will be, and this kind of thing, and we'll end it like this is that that assumes there's a human participant, but if its algorithms and code that's responding, code against code, do you hold the code writers responsible? Who ultimately will become the responsible entity for that phenomenon? So, on that cheerful note, maybe an appendix to the Manual. *[humorously]*

MR. MCCORMACK: Another thousand pages!

[AUDIENCE LAUGHTER]

MR. RISHIKOF: I'll give our panelists a last moment or a last word if they want to say anything? Nick?

DR. ROSTOW: No, I think I've said enough!

[AUDIENCE LAUGHTER]

MR. BOWMAN: I think I've said enough too!

[AUDIENCE LAUGHTER]

MR. MCCORMACK: I just thank you for your attention and if you have any questions please feel free to ask.

MR. RISHIKOF: So last, Mrs. McCormack do you have a last question that you want to pose? *[humorously]*

[AUDIENCE LAUGHTER]

No! In that case, we will then end the evening. I want to thank the journal for putting on this wonderful forum and supplying this, a great opportunity for us to discuss it. Thank you so much!

MR. MYERS: Thank you. Well, on behalf of the *National Security Law Journal* I'd like to thank our panelists and moderator: Mr. McCormack, Dr. Rostow, Mr. Bowman, and Mr. Rishikof. Thank you for taking time to join us tonight.

I'd like to recognize our Symposium Editor, Kirstin Riesbeck, there in the back, who put this on. It was a very good event. And at this time I'd encourage everyone to join us back in the gallery. I think there's still some food and drinks available. Thank you!

COMMENT

THE REVIVAL OF TREASON: WHY HOMEGROWN TERRORISTS SHOULD BE TRIED AS TRAITORS

Jameson A. Goodell*

The rise of the Islamic State of Iraq and the Levant (ISIL) has led to unprecedented levels of American recruits seeking to further ISIL's agenda by both carrying out attacks on the homeland and traveling overseas to support extremist efforts there. In response, the United States government prosecuted these individuals mostly under charges of seditious conspiracy or material support to designated terrorist organizations. However, these charges do not accurately reflect the true nature of the crimes committed by homegrown terrorists: a betrayal of the United States by sympathizing with and supporting the nation's enemies. The only charge that appropriately acknowledges this betrayal of allegiance is the charge of treason. Treason punishes those who, owing allegiance to the United States, levy war against the nation, or in adhering to its enemies, gives them aid and comfort. This accurately describes the crimes homegrown terrorists commit when they support foreign terrorist organizations. Treason is the most appropriate charge for prosecuting these individuals because it acknowledges the sense of national allegiance and solidarity against the nation's enemies, provides an adequate punishment that fits the severity of the crime, and avoids constitutional issues associated with the currently enforced statutes under the rule against constructive treasons.

* George Mason University School of Law, Juris Doctor Candidate, May 2017; Virginia Military Institute, B.A., International Studies & Arabic Language and Culture, 2014.

INTRODUCTION

On January 21, 2015, the United States Department of Justice indicted Christopher Cornell, a 20-year-old American citizen from Green Township, Ohio,[1] for attempting to kill an officer of the United States, solicitation to commit a crime of violence, and possession of a firearm in furtherance of a crime of violence.[2] About four months later, the prosecution added an additional charge of attempting to provide material support to the Islamic State of Iraq

[1] Press Release, U.S. Dep't of Justice: Office of Pub. Affairs, Cincinnati-Area Man Charged with Attempting to Provide Material Support to ISIL (May 7, 2015) [hereinafter Cornell Press Release], http://www.justice.gov/ opa/pr/cincinnati-area-man-charged-attempting-provide-material-support-isil. Because this is an ongoing criminal investigation, this comment is in no way a statement on the guilt or innocence of the accused, who is presumed innocent until proven guilty in a court of law. *See id.*

[2] *See id.*; Kimball Perry, *Terror Suspect Wants to be Called 'Mr. Ubaydah'*, USA TODAY (Jan. 16, 2015), http://www.usatoday.com/story/news/nation/2015/01/16/terror-suspect-arraignment/21868735/.

and the Levant ("ISIL", also known as ISIS).[3] Allegedly, Cornell had discussed his intent to construct bombs and attack the United States Capitol in Washington, D.C. with an informant from the Federal Bureau of Investigation ("FBI").[4] Cornell told the informant that the attacks would be on behalf of ISIL, as part of his jihad against the United States.[5] Cornell was arrested after leaving a gun store where he purchased two semi-automatic rifles and 600 rounds of ammunition to use in his attack.[6]

On September 9, 2015, Hanad Mustofe Musse, a 19-year-old American citizen from Minneapolis, Minnesota, pleaded guilty to conspiring to provide material support to ISIL.[7] Musse, along with eight other co-conspirators, planned to travel overseas to join ISIL in Syria, however, police thwarted the plan in November 2014.[8] Following this failed attempt, police arrested Musse a second time after he attempted to obtain a false passport, and continued to meet with his co-conspirators. The United States charged him with conspiracy to provide material support to a known terrorist organization.[9]

Had either of these crimes come to fruition, the consequences in terms of loss of life and furthering ISIL's agenda would have been severe, such as a potential attack on the U.S. Capitol Building. These crimes were attempts by U.S. citizens, who were supporting an enemy of the United States,[10] to further that enemy's objectives in the form of warlike actions against the United States

[3] Cornell Press Release, *supra* note 1.
[4] Criminal Complaint at 3-5, United States v. Cornell (S.D. Ohio filed Jan. 14, 2015) (No. 1:15-mj-24).
[5] *Id.*
[6] *Id.* at 5.
[7] Press Release, U.S. Dep't of Justice: Office of Pub. Affairs, Minneapolis Man Pleads Guilty to Conspiracy to Provide Material Support to ISIL (Sept. 9, 2015) [hereinafter Musse Press Release], https://www.fbi.gov/ minneapolis/pressreleases/2015/ Minneapolis-man-pleads-guilty-to-conspiracy-to-provide-material-support-to-isil.
[8] *Id.*
[9] *Id.*
[10] *See* Ceylan Yeginsu & Helene Cooper, *U.S. Jets to Use Turkish Bases in War on ISIS*, N.Y. TIMES (July 23, 2015), http://www.nytimes.com/2015/07/24/world/ europe/turkey-isis-us-airstrikes-syria.html?_r=0 (explaining how U.S. is conducting military operations against ISIS targets in Syria and is a threat to the United States).

and its allies. These actions are a betrayal of the country whose laws have protected these people their entire lives. Only one charge adequately punishes these actions: treason.

Treason is the only crime defined in the United States Constitution, stating: "Treason against the United States, shall consist only in levying War against them, or in adhering to their Enemies, giving them Aid and Comfort . . . ."[11] Though the last treason trial in the United States took place in 1952,[12] the crime remains especially relevant during the War on Terror, where more and more U.S. citizens have sought to support foreign terrorist organizations ("FTO").[13]

Since the beginning of the War on Terror, the United States treated terrorism as a crime, punishable by the laws enacted by Congress, mostly involving charges of seditious conspiracy or providing material support to terrorist organizations. However, when a U.S. citizen commits these crimes, the offense carries an extra degree of severity: a betrayal of the allegiance a citizen owes their country.[14] Treason is the only charge that properly vindicates allegiance while providing an appropriate punishment that fits the severity of the crime committed, and avoids the constitutional issues associated with the current statutory scheme. For these reasons, the United States should revive treason as a more commonly used tool to prosecute and punish U.S. citizens who engage with and support the enemies of the United States.

Part I of this Comment will provide background information regarding the elements of treason as defined by the Treason Clause of

---

[11] U.S. CONST. art. III, § 3, cl. 1.

[12] Suzanne Kelly Babb, *Fear and Loathing in America: Application of Treason Law in Times of National Crisis and the Case of John Walker Lindh*, 54 HASTINGS L. J. 1721, 1743 (2003).

[13] Wesley Bruer, *Study: Unprecedented Support for ISIS in the U.S.*, CNN (Dec. 2, 2015, 11:48 AM), http://www.cnn. com/2015/12/01/politics/isis-in-united-states-research/; Ed Payne, *More Americans Volunteering to Help ISIS*, CNN (Mar. 5, 2015, 4:55 PM), http://www.cnn.com/2015/03/05/us/isis-us-arrests/. *See generally*, LORENZO VIDINO & SEAMUS HUGHES, ISIS IN AMERICA: FROM RETWEETS TO RAQQA iv (2015).

[14] Carlisle v. United States, 83 U.S. 147, 154 (1872).

the Constitution and the history and ramifications behind treason's constitutional posture. Part II will examine the current statutory scheme for terrorism prosecutions, emphasizing the seditious conspiracy and material support statutes while comparing them to the elements of treason. Part III will apply the principles of the Treason Clause to the Cornell and Musse cases to demonstrate that the United States can use treason to prosecute homegrown terrorist activities. Part IV will argue that treason is a more appropriate charge than the current statutory scheme, first by detailing the positive benefits that labeling individuals as traitors has on society, and second by addressing the constitutional issues the current statutes face.

I. TREASON: ELEMENTS AND HISTORY

The Treason Clause reads:

> Treason against the United States, shall consist only in levying War against them, or in adhering to their Enemies, giving them Aid and Comfort. No Person shall be convicted of Treason unless on the Testimony of two Witnesses to the same overt Act, or on Confession in open Court. The Congress shall have Power to declare the Punishment of Treason, but no Attainder of Treason shall work Corruption of Blood, or Forfeiture except during the Life of the Person attainted.[15]

Under the Clause, a person can commit treason in two ways: (1) by levying war against the United States; or (2) by adhering to enemies of the United States, by giving them aid and comfort. A charge of treason requires three elements: an allegiance to the United States, the commission of overt acts that are treasonous in nature, and either the testimony by two witnesses to each overt act, or the confession of the accused in open court.[16] Because of the nature of the Clause as a constitutional provision, the wording is unlikely to be changed, and any changes must come by means of interpretation. The following sections will describe the elements of treason in detail

---

[15] U.S. CONST., art. III, § 3, cl. 1.

[16] *See* Treason, 18 U.S.C. § 2381 (1994) ("[w]hoever, owing allegiance to the United States, levies war . . . ."); Cramer v. United States, 325 U.S. 1, 30 (1945).

and how the Supreme Court has interpreted them, as well as the history behind why the Founders included the Treason Clause in the Constitution.

A. Elements of Treason

In order to define the various elements of treason, one must look to the leading court cases that have reviewed the Treason Clause.

1. Allegiance

The first element that is inherent in the charge of treason, but not expressly stated in the Clause, is the element of allegiance. Treason historically has been a crime of betraying allegiance.[17] The First Congress in its codification of the Treason Clause included the allegiance element as part of the offense,[18] even though the Treason Clause did not specifically require allegiance as an element of the offense. The allegiance element could also be derived from the phrase "against the United States," which indicates that an individual must owe some duty to the United States for a crime to be treasonous.

When the accused is a United States citizen, the allegiance element is automatically established.[19] There is no territorial limitation to this, meaning, "[a]n American citizen owes allegiance to the United States wherever he may reside."[20] If a United States citizen commits a treasonous action abroad, they remain subject to prosecution for that action in U.S. courts. The Court in *Kawakita v. United States* faced the issue of whether a person, born in the United States to Japanese nationals, retained his United States citizenship when he traveled to Japan, and while working as an interpreter for

---

[17] *See* Note, *Historical Concept of Treason: English, American*, 35 IND. L. J. 70, 70 (1959) (explaining that early Roman concept of treason included betrayal of community allegiance).

[18] An Act for the Punishment of certain Crimes against the United States, 1 Stat. 112, § 1 (1790).

[19] Kawakita v. United States, 343 U.S. 717, 734 (1952) ("American citizenship, until lost, carries obligations of allegiance as well as privileges and benefits.").

[20] *Id.* at 736.

the Japanese military, subjected American prisoners of war to cruel and humiliating conditions.[21] As a matter of naturalization and international law, the Court held Kawakita had dual citizenship and had retained his United States citizenship.[22] Thus, he still retained allegiance to the United States and was triable for treason.[23]

Even foreign nationals, who are temporarily within the country owe a temporary allegiance, and the government may try them for treason.[24] In *Carlisle v. United States*, the United States charged British citizens with treason stemming from their manufacturing and sale of saltpeter to the Confederate military while in the United States.[25] The major issue in the case was whether President Andrew Johnson's general pardon of those involved in the rebellion during the Civil War included the foreign aliens involved, but the Court announced this broad definition of allegiance and found the aliens were still chargeable with treason.[26]

Thus, the allegiance element is simple and well defined. All U.S. citizens, wherever they may be, owe allegiance to the United States until they perform the legal requirements necessary to renounce their citizenship. Additionally, any foreign national who temporarily resides in the United States, owes a temporary allegiance to the country and is triable for acts of treason occurring within the United States.

2. Levying War

Levying war has been defined as the "direct effort to overthrow the government, or wholly to supplant its authority in some part or all of its territory."[27] The most important aspect of the crime of levying war has been the requirement that there must be an

[21] *Id.*
[22] *Id.* at 733-36
[23] *Id.*
[24] Carlisle v. United States, 83 U.S. 147, 154 (1872).
[25] *Id.* at 150.
[26] Carlton F.W. Larson, *The Forgotten Constitutional Law of Treason and the Enemy Combatant Problem*, 154 U. PA. L. REV. 863, 891-92 (2006).
[27] Willard Hurst, *Treason in the United States*, 58 HARV. L. REV. 806, 823 (1945) [hereinafter Hurst's Treason Part III].

assemblage of persons for executing a treasonous design.[28] The assemblage requirement is necessary because it was factually impossible for a single individual to levy war at the time of the Founding.[29] This principle is overshadowed by the fact that now a single individual with a nuclear weapon could cause a massive amount of destruction, but nonetheless assemblage remains the lynchpin on the levying war provision.[30]

However, this is distinguished from a mere conspiracy to levy war. The cases of *Ex parte Bollman* and *United States v. Burr* both revolved around Aaron Burr's alleged conspiracy to attack Spanish Mexico and cities in the Louisiana Territory in order to separate them from the rest of the United States.[31] The Court in *Bollman* stated, "[t]o conspire to levy war, and actually to levy war, the distinct offences. The first must be brought into operation by the assemblage of men for a purpose treasonable in itself, or the fact of levying war cannot have been committed."[32] The Court held that mere intent to assemble and mere enlistment of people does not amount to levying war, but

> [I]f a body of men be actually assembled for the purpose of effecting by force a treasonable purpose, all those who perform any part, however minute, or however remote from the scene of action, and who are actually leagued in the general conspiracy, are to be considered as traitors.[33]

Treason by levying war requires an assemblage of people with treasonable purpose, who have attained some capability of force that amounts to levying war. However, a show of force can be ambiguous. Chief Justice John Marshall, who presided over the treason trial of Aaron Burr, admitted assemblages need not be armed, nor fire a shot:

---

[28] *Ex parte* Bollman, 8 U.S. 75, 127 (1807).
[29] *See* United States v. Burr, 25 F. Cas 55, 169 (C.C.D. Va. 1807) (Marshall, C.J).
[30] Randel J. Meyer, *The Twin Perils of the Al-Aulaqi Case: The Treason Clause and the Equal Protection Clause*, 79 BROOK. L. REV. 229, 248 (2013).
[31] Larson, *supra* note 26, at 907.
[32] *Ex parte* Bollman, 8 U.S. at 126.
[33] *Id.*

> If a rebel army, avowing its hostility to the sovereign power . . . should march and countermarch before it, should manoeuvre in its face, and should then disperse from any cause whatever without firing a gun—I confess I could not, without some surprise, hear gentlemen seriously contend that this could not amount to an act of levying war.[34]

This suggests treason by levying war does not require a consummated act of war, but rather an assemblage gathered with the intent and force necessary to engage in war.

3. Adhering to their Enemies, Giving them Aid and Comfort

Traditionally, the U.S. courts have interpreted "aid and comfort" to require an act that is "directed in furtherance of the hostile designs of the enemies of the United States" and "strengthens, or tends to strengthen, the enemies of the United States." [35] Moreover, "an act which weakens, or tends to weaken, the power of the United States to resist or to attack the enemies of the United States . . . is in law giving aid and comfort . . . ."[36] Because there need not be an "actual blow" to the United States, the Treason Clause has been interpreted as prohibiting actions whose natural effects are strengthening an enemy.[37] Acts that clearly provide aid and comfort are those such as sending provisions, money, furnishing arms, or giving intelligence to an enemy.[38] Courts drew a line however, holding that words spoken, written, or printed were insufficient to satisfy the element.[39]

The Supreme Court in *Cramer v. United States* changed the traditional natural effects rule to require that the accused must

---

[34] United States v. Burr, 25 F. Cas. 55, 162 (C.C.D. Va. 1807) (No. 14693) (Marshall, C.J.).
[35] United States v. Fricke, 259 F. 673, 676 (S.D.N.Y. 1919).
[36] *Id.*
[37] *See In re* Charge to Grand Jury, 30 F. Cas. 1046, 1047 (C.C.D. R.I. 1842) (No. 18275) (Story, J.).
[38] *Id.* at 1035.
[39] *Id.*

actually have given aid and comfort.[40] The Court stated, "[t]he very minimum function that an overt act must perform in a treason prosecution is that it show sufficient action by the accused, in its setting, to sustain a finding that the accused actually gave aid and comfort to the enemy."[41] The prosecution alleged that Anthony Cramer met with individuals he knew to be German saboteurs in a New York City bar and aided them.[42] The Court held that this action alone may have been sufficient to prove a treasonous intent, but was not sufficient to prove that he actually provided aid and comfort to the enemy saboteurs.[43]

The *Cramer* opinion has received a considerable amount of criticism, particularly from Willard Hurst, author of the seminal treatise on treason law prior to 1945. Hurst argued the *Cramer* Court created bad law, and confused the subject.[44] Hurst claims the majority advanced no justification or authority for the proposition that actual aid be given and "[t]o wait for aid to be 'actually' given the enemy risks stultification: the treason may be successful to the point at which there will no longer be a sovereign to punish it."[45] He also recognized the treason charge's value in prevention as well as punishment.[46]

Conventional wisdom would suggest that the majority in *Cramer* intended for treason prosecutions to be rare and difficult to prove.[47] However, in the decade following *Cramer*, about a dozen treason prosecutions went to trial, all of which but one resulted in convictions affirmed on appeal.[48] Thus, prosecutors could still prove treason under the *Cramer* rule. In fact lower courts on multiple occasions affirmed treason convictions for people engaged in radio

[40] Cramer v. United States, 325 U.S. 1, 34-35 (1945).
[41] *Id.*
[42] *Id.* at 36.
[43] *Id.* at 39, 48.
[44] Hurst's Treason Part III, *supra* note 27, at 806.
[45] *Id.* at 836-37.
[46] *Id.* at 837.
[47] Paul T. Crane, *Did the Court Kill the Treason Charge? Reassessing* Cramer v. United States *and its Significance*, 36 FLA. ST. U. L. REV. 635, 675 (2009).
[48] *Id.* at 677-78.

propaganda for enemy governments.[49] This, in essence, reversed the old idea that words alone cannot be the overt act that aids and comforts the enemy. Words retain a criminal character when they "constitute acts in furtherance of a program of an enemy to which the speaker adheres and to which he gives aid with intent to betray his own country."[50] The Supreme Court has not had the opportunity to rule on what became of the *Cramer* rule, as there has not been a treason case to review since 1954.[51]

4. Testimony of Two Witnesses to the Same Overt Act

As an evidentiary matter, a treason prosecution requires at least two witnesses to testify to each overt act alleged. This does not mean that the testimony of both witnesses must be identical, but must be to the same general act.[52] In *Haupt v. United States*, multiple witnesses saw the defendant's son, a German saboteur, enter the defendant's apartment building and saw him inside the defendant's apartment, but never saw him physically enter the apartment and remain overnight.[53] The Court held that, though two witnesses did not testify to the same precise overt act, the witnesses collectively testified that the defendant was keeping his son sheltered in his apartment and provided him aid and comfort.[54]

Though at least two witnesses must corroborate physical overt acts, the Court has held the intent aspect of adherence to the enemy would be impossible to prove by direct witnesses.[55] Thus "it is permissible to draw usual reasonable inferences as to intent from the overt acts," because every person intends the natural consequences of

[49] *See* Burgman v. United States, 188 F.2d 637 (D.C. Cir. 1951), *cert. denied*, 342 U.S. 838 (1951); Chandler v. United States, 171 F.2d 921 (1st Cir. 1948), *cert. denied*, 336 U.S. 918 (1949).
[50] Gillars v. United States, 182 F.2d 962, 971 (D.C. Cir. 1950).
[51] Crane, *supra* note 47, at 675.
[52] *See* Haupt v. United States, 330 U.S. 631, 640 (1947).
[53] *Id.* at 636-38.
[54] *Id.* at 637-38.
[55] Cramer v. United States, 325 U.S. 1, 31 (1945) ("[i]f we were to hold that the disloyal and treacherous intention must be proved by the direct testimony of two witnesses, it would be to hold that it is never provable.").

their behavior.[56] Thus a jury can infer treasonous intent from the overt acts testified by two witnesses without any further testimony indicating the state of mind of the accused.

5. Confession in Open Court

A treason conviction can also result if the accused confesses to the crime in open court. There has only been one instance in American history where an individual has pleaded guilty and confessed to treason in open court.[57] This does not mean that any admissions made by the accused to agents outside of court can suffice as "confessions in open court," nor can they supply a deficiency in proving the overt act itself.[58]

B. Treason Clause History and the Rule Against Constructive Treason

The Treason Clause was largely derived from English and colonial definitions of the crime.[59] English law had long defined treason in a fashion similar to what became the Constitutional Treason Clause.[60] The Statute of Edward III defining treason reads in relevant part, "[I]f a Man do levy War against our Lord the King in his Realm, or be adherent to the King's Enemies in his Realm, giving them Aid and Comfort in the Realm, or elsewhere . . . ought to be Judged Treason."[61]

This wording provided a significant basis for the modern constitutional Treason Clause. This is so because the Framers at the

---

[56] *Id.*
[57] The defendant was a U.S. Army Sergeant who had stolen an airplane, flew to Germany, and helped the German military by providing radio propaganda against American forces. United States v. Monti, 168 F. Supp. 671, 672 (E.D.N.Y. 1958). In light of several similar treason cases upheld on appeal, Monti's lawyers advised him to plead guilty and confess in open court in order to obtain a lesser sentence. *See* United States v. Monti, 100 F. Supp. 209, 213 (E.D.N.Y. 1951).
[58] *Cramer*, 325 U.S. at 44-45.
[59] *See* Willard Hurst, *Treason in the United States*, 58 HARV. L. REV. 226, 400 (1944).
[60] *See* Treason Act 1351, 25 Edw. 3 c. 2 § 5 (Eng.), http://www.legislation.gov.uk/aep/Edw3Stat5/25/2#commentary-c919019.
[61] *Id.*

Constitutional Convention weighed the results of inserting the "Aid and Comfort" provision as a limiting function on "Adhering to the Enemy."[62] Deciding that the adhering element was too indefinite on its own, the Framers inserted "aid and comfort" as a restrictive provision.[63] Rufus King, a Massachusetts representative at the Convention, noted skepticism over the importance of the Clause, because Congress could levy capital punishment under other names than Treason.[64] This was not the view of the other Framers who sought to put closer limits on the crime.[65]

Another point of contention in the adoption of the Treason Clause was the juxtaposition of the overt act element with the two-witness requirement. The Framers did this because the overt act was meant to constitute a distinct element of proof that is directly linked to the two-witness rule.[66] The Framers derived the two-witness requirement from another English statute, 7 William III, which provided stronger evidentiary protection and guarded against perjury of witnesses.[67]

The Framers' intent for including the Treason Clause within the Constitution was to immortalize the definition, thus preventing a rogue legislature from creating what James Madison called "new-fangled and artificial" treasons.[68] These judge-made expansions of the common law definition of treason, more commonly called "constructive treasons," were made in order to cover conduct that had never before been known as treasonous.[69] This was a common practice in England and is what prompted the passage of the Statute

[62] Willard Hurst, *Treason in the United States*, 58 HARV. L. REV. 395, 399-402 (1945) [hereinafter Hurst's Treason Part II].
[63] *Id.* at 402.
[64] *Id.* at 400-01.
[65] *Id.* at 401.
[66] *Id.* at 403.
[67] Jon Roland, *Hurst's Law of Treason*, 35 UWLA L. REV. 297, 298 (2003); Hurst's Treason Part II, *supra* note 62, at 403.
[68] THE FEDERALIST NO. 43 (James Madison).
[69] Meyer, *supra* note 30, at 237.

of Edward III in order to control the definition of treason by the legislature instead of the courts.[70]

Another major concern was that the state could use an undefined definition of treason to punish political dissidents or people who opposed the sovereign's policies. Based on the freedom of speech and freedom of peaceful political expression, later memorialized in the First Amendment, it was important to limit the definition of treason to only levying war and adhering to enemies of the United States by providing aid and comfort to them.[71] The Statute of Edward III included as treason, "compass[ing] or imagin[ing] the Death of our Lord the King."[72] This led to some extreme treason convictions that were unacceptable to the Framers.[73] They believed that treason required a limited definition so that a creative legislature could not criminalize as treason political speech or opposition to the government or its policies.[74]

These themes became what is known as the "rule against constructive treasons," which is that Congress cannot make immaterial variations in the elements of treason that leave the gravamen of the offense intact without providing the procedural protections the Treason Clause provides.[75] Early cases applying the Treason Clause adopted this rule. In *Ex parte Bollman*, Chief Justice Marshall stated:

> It is therefore safer as well as more consonant to the principles of our constitution, that the crime of treason should not be extended by construction to doubtful cases; and that crimes not clearly within the constitutional definition, should receive

[70] Hurst's Treason Part II, *supra* note 62, at 409.
[71] *Id.* at 430.
[72] Treason Act 1351, *supra* note 60.
[73] *See* Hurst's Treason Part II, *supra* note 62, at 409 n.101 (describing a conviction of treason for wishing the death of the King after the king killed the accused's favorite buck).
[74] *See id.* at 414.
[75] Meyer, *supra* note 30, at 239.

> such punishment as the legislature in its wisdom may provide.[76]

Chief Justice Marshall suggests that if a crime clearly falls within the constitutional definition of treason, then the legislature may not create a statute criminalizing the same conduct.

However, no court has invalidated a law for violating the rule against constructive treasons. The first time this argument came upon the courts was in regards to the Espionage Acts of 1917 and 1918, but the decisions did not adequately rule on this issue.[77] In fact, the Supreme Court decisions facing this issue did not rule either way on the claim.[78] The only mention of the treason clause comes from Justice Brandeis' dissenting opinion in *Schaefer*, joined by Justice Holmes, which stated, "[t]o prosecute men for such publications reminds of the days when men were hanged for constructive treason. And, indeed, the jury may well have believed from the charge that the Espionage Act had in effect restored the crime of constructive treason."[79]

The most reasoned consideration of the rule against constructive treason argument during the post-World War I era is found in the Sixth Circuit's opinion in *Wimmer v. United States*. The court distinguished the Espionage Act saying that it punished "adherence by words" which was different from an overt act giving aid and comfort to an enemy.[80] However, the court noted that "[i]f we had to do with a case where the conduct which was prosecuted consisted of acts, we would have to consider the line of reasoning upon which *Wimmer* depends."[81] Notably, these cases were decided before courts held that providing enemy propaganda through speech

---

[76] *Ex parte* Bollman, 8 U.S. 75, 127 (1807).
[77] *See* Hurst's Treason Part II, *supra* note 62, at 438-42.
[78] *See* Schaefer v. United States, 251 U.S. 466 (1920) (no mention of treason in majority opinion); Frohwerk v. United States, 249 U.S. 204, 210 (1919) (dismissing argument out of hand).
[79] *Schaefer*, 251 U.S. at 493 (Brandeis, J., dissenting).
[80] Wimmer v. United States, 264 F. 11, 13 (6th Cir. 1920).
[81] *Id.* at 12.

could provide aid and comfort, even under the restrictive *Cramer* rule.[82]

The landmark case of *Ex parte Quirin* was the final time the constructive treason argument was seen before the Treason Clause fell out of use. However, similar to the issue's treatment of the issue in *Frohwerk*, the Court summarily dismissed the subject with little discussion. The case involved German saboteurs (one of whom may have been a United States citizen, who had entered the United States to conduct sabotage missions) who had abandoned their German uniforms upon arrival.[83] The United States captured the saboteurs and charged them under a military commission for violations of the laws of war, specifically for abandoning their uniforms and planning to attack the United States.[84] The Court distinguished this offense from that of treason only by way of the absence of uniform element:

> The offense was complete when with that purpose they entered-or, having so entered, they remained upon-our territory in time of war without uniform or other appropriate means of identification. For that reason, even when committed by a citizen, the offense is distinct from the crime of treason defined in Article III, s 3 of the Constitution, since the absence of uniform essential to one is irrelevant to the other.[85]

However, even though absence of a uniform is not an element of treason, it does not change that what these saboteurs did could constitute levying war under the Treason Clause.

The strongest statement from the Court in derogation of the rule against constructive treason came from *Cramer*. The Court recognized that Congress could not rid itself of the two-witness requirement by merely giving treason another name, but gave Congress wide latitude in "enact[ing] prohibitions of specified acts thought detrimental to our wartime safety."[86] The Court noted that prosecutors could wish to avoid the "passion-rousing" potential of

---

[82] *See e.g.*, Gillars v. United States, 182 F.2d 962, 971 (D.C. Cir. 1950).
[83] *Ex parte* Quirin, 317 U.S. 1, 20-22 (1942).
[84] *Id.* at 23, 31.
[85] *Id.* at 38.
[86] Cramer v. United States, 325 U.S. 1, 45 (1945).

treason prosecutions and instead focus upon a defendant's specific intent to do particular acts different from the definition of treason.[87] This statement from the Supreme Court along with the general practice of prosecutorial discretion, in large part explains the disappearance of treason prosecutions following the World War II era.[88]

Despite its ill-treatment, the rule against constructive treasons still remains, and was an important consideration the Framers made when they included the Treason Clause within the Constitution, instead of leaving the definition of the crime to the whims of Congress.

II. MODERN ENFORCEMENT OF TERRORIST ACTIVITIES

Following the *Cramer* decision and the disuse of treason prosecutions, Congress was free to prohibit subversive conduct without having to comply with the procedural protections of the Treason Clause. This has led to a large number of criminal statutes that prosecutors have used to combat terrorism at home and abroad. The following sections will detail the most commonly used of these statutes as well as the nature of modern homegrown terrorism.

A. Current Statutory Scheme

Today, there are a wide array of criminal punishments for conduct relating to aiding foreign entities, governments, and enemies of the United States or levying war against the United States.[89] Since the treason charge has fallen into disuse, many of these statutes have become the norm for prosecution of terrorism-related activities in the United States. Because of the large number of criminal laws that punish potentially treasonable conduct, this Comment's focus will be

---

[87] *Id.*

[88] *See* Crane, *supra* note 47, at 682.

[89] *See, e.g.*, Gathering or Delivering Defense Information to Aid Foreign Government, 18 U.S.C. § 794 (1996); Providing Material Support or Resources to Designated Foreign Terrorist Organizations, 18 U.S.C. § 2339B (2015); Seditious Conspiracy, 18 U.S.C. § 2384 (1994); Recruiting for Service Against United States, 18 U.S.C. § 2389 (1994).

concentrated on the most enforced statutes: 18 U.S.C. §§ 2339A-B (providing material support to terrorists) and 18 U.S.C. § 2384 (seditious conspiracy).

1. Material Support to Designated Foreign Terrorist Organizations

Section 2339B reads in relevant part:

> Whoever knowingly provides material support or resources to a foreign terrorist organization, or attempts or conspires to do so, shall be fined under this title or imprisoned not more than 20 years, or both, and, if the death of any person results, shall be imprisoned for any term of years or for life. To violate this paragraph, a person must have knowledge that the organization is a designated terrorist organization . . . .[90]

Section 2339A defines "material support or resources" as:

> . . . any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself), and transportation, except medicine or religious materials.[91]

In brief, the statute criminalizes providing material support, including money, personnel, and weapons, to designated FTOs with the only scienter requirement being knowledge of the terrorist organization's status.

Under the statute, many of the same items that constitute "material support" are identical to those which courts have found provided "aid and comfort" to enemies in treason prosecutions.[92]

---

[90] 18 U.S.C. § 2339B(a)(1).

[91] Providing Material Support to Terrorists, 18 U.S.C. § 2339A(b)(1) (2009).

[92] *Compare* 18 U.S.C. § 2339A(b)(1), *with* Gillars v. United States, 182 F.2d 962, 971 (D.C. Cir. 1950), *and* Haupt v. United States, 330 U.S. 631, 640 (1947) (providing provisions, money, arms, and intelligence provides aid and comfort).

Every item listed in the statute can be considered a form of aid or comfort provided to a terrorist organization. The definition of aid or comfort may be more expansive under the Treason Clause as evidenced by later cases finding war propaganda in support of an enemy as treasonous.[93]

The major difference between the material support statutes and the Treason Clause is that treason focuses on the amorphous term "enemies of the United States" while material support only applies to designated FTOs. However different the two terms are, the difference is subtle. It can hardly be said that terrorist organizations the United States is actively engaged in combat with are not "enemies of the United States."[94] Further, U.S. courts have never required a formal declaration of war or even a formal authorization of military force for a foreign country or organization to become an "enemy" of the United States.[95] As long as circumstances are such that Congress and the executive agree that a foreign country or organization is an enemy, then they are an enemy.[96] All designations of FTOs require a finding by the Secretary of State that the organization's terrorist activity threatens the security of U.S. nationals or U.S. national security.[97] If the government properly designates a terrorist organization, and the organization does pose such a threat to national security, then the United States can consider them "enemies." This remains true even if the United States is not engaged in active military operations against them.

---

[93] *See* Burgman v. United States, 188 F.2d 637, 639 (D.C. Cir. 1951); Chandler v. United States, 171 F.2d 921, 942-43 (1st Cir. 1948).

[94] *See* Authorization for Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (2001) (authorizing use of military force against perpetrators of September 11 attacks); *see also* Amber Phillips, *President Obama's Push for Military Authorization to Fight ISIS Won't go Anywhere in Congress. Here's Why.*, WASH. POST (Dec. 7, 2015), https:// www.washingtonpost.com/news/the-fix/wp/2015/12/07/3-reasons-congress-wont-authorize-obamas-use-of-force-against-the-islamic-state/ (explaining President Obama believes we are at war with ISIL).

[95] *See* Bas v. Tingy, 4 U.S. 37, 41 (1800) (finding France to be an "enemy" despite no formal declaration of war); Orlando v. Laird, 443 F.2d 1039, 1043 (2d Cir. 1971) (holding Congress acted sufficiently to authorize war in Vietnam without formal declaration).

[96] *See Bas*, 4 U.S. at 41.

[97] Designation of Foreign Terrorist Organizations, 8 U.S.C. § 1189(c) (2004).

A designation would show both Congress and the President's agreement that the organization poses a threat to the United States and any support given to them, regardless of its intended use, is prohibited. Based on these factors, the government could properly label any terrorist organization as an "enemy" of the United States. Especially following the November 13, 2015 attacks on Paris and the ISIL-inspired attack in San Bernardino, California, it is reasonable to conclude that ISIL is an "enemy" of the United States. It is also important to note there is a proposed amendment to the treason statute, 18 U.S.C. § 2381, to make any designated FTO an enemy of the United States for purposes of treason.[98]

2. Seditious Conspiracy

The other criminal charge most used to prosecute terrorism cases is 18 U.S.C. § 2384 for seditious conspiracy. Section 2384 reads:

> If two or more persons in any State or Territory, or in any place subject to the jurisdiction of the United States, conspire to overthrow, put down, or to destroy by force the Government of the United States, or to levy war against them, or to oppose by force the authority thereof, or by force to prevent, hinder, or delay the execution of any law of the United States, or by force to seize, take, or possess any property of the United States contrary to the authority thereof, they shall each be fined under this title or imprisoned not more than twenty years, or both.[99]

This statute punishes the conspiracy to use force to overthrow or levy war against the government. One of the major purposes of this law is that it enables the government to arrest and prosecute a suspected terrorist before any substantive crime has occurred.[100] The Government need not wait for buildings to be bombed or lives to be lost before arresting and prosecuting conspirators under this law.[101]

---

[98] *See* H.R. 2020, 114th Cong. (2015); S. 542, 114th Cong. (2015).
[99] 18 U.S.C. § 2384 (1994).
[100] United States v. Rahman, 189 F.3d 88, 116 (2d Cir. 1999).
[101] *Id.*

However noble this purpose, it does not change the fact that this statute punishes conspiracy to levy war or use force against the United States, which is also punishable as treason. As discussed in Part I, all that is required to constitute "levying war" is an assemblage of people who have both traitorous intent and the capabilities to use force that amounts to levying war.[102] Although a pure conspiracy without action is different from actually levying war, many conspiracies also fall under the Treason Clause, as long as there are multiple people involved and they have plans and materials to carry out an attack. Based on this notion, using the Treason Clause as grounds for prosecution accomplishes the same goal as the seditious conspiracy statute.

3. Rule Against Constructive Treason Applied

Both the material support and seditious conspiracy statutes punish conduct that is also punishable under the Treason Clause. This conflict implicates the rule against constructive treasons, which would invalidate these laws. However, on only a few occasions has a reviewing court been faced with a rule against constructive treason argument, and in each case, the courts dismissed the argument and upheld the statutes.

The first time a defendant used the constructive treason argument against one of these statutes was *United States v. Rodriguez*.[103] This case dealt with a seditious conspiracy conviction arising from a plot to bomb military training centers in Illinois.[104] The defendant challenged Section 2384, arguing it was a constructive treason and dispensed with the two witness requirement.[105] The court rejected this argument, holding that Section 2384 protected different government interests and proscribed a different crime.[106] The court distinguished Section 2384 from treason because seditious conspiracy does not require an allegiance element, does not extend beyond jurisdictional boundaries, and a conspiracy requires at least

[102] *See* Hurst's Treason Part III, at 823.
[103] United States v. Rodriguez, 803 F.2d 318, 320 (7th Cir. 1986).
[104] *Id.* at 319.
[105] *Id.* at 320.
[106] *Id.*

two persons.[107] The court also distinguished these two because they served different purposes: preventing urban terrorism for seditious conspiracy as opposed to punishing traitors for treason.[108]

Constructive treason arose again as an issue in *United States v. Rahman*.[109] The defendant in this case challenged the seditious conspiracy statute on the same grounds as in *Rodriguez* and the court rejected the argument in a similar fashion.[110] The court expressly declined to answer the question whether the government could charge a defendant with subversive conduct, a crime with all the same elements as treason except the two-witness requirement.[111] The court did this because it distinguished the crime of seditious conspiracy and treason on the allegiance element alone.[112]

The last time courts saw the argument was *United States v. Augustin*, where the defendant challenged an amendment to his indictment under the material support statutes.[113] In a brief review of the matter, the court rejected his argument, finding that the material support statute did not include allegiance to the United States as an element of the offense, citing both *Rahman* and *Rodriguez*.[114]

These courts failed to recognize that the differences they observed were covered under the elements of treason. Allegiance, as discussed above, is a non-factor when it pertains to U.S. citizens or aliens residing in the United States, which covers each one of the defendants in those cases.[115] Additionally, levying war requires an assemblage of persons, so a conspiracy of two or more people can fall under this definition. The court in *Rahman* almost recognizes that a conspiracy to use force against the United States is the same as treason, only distinguishing the two based on the allegiance

[107] *Id.*
[108] *Id.*
[109] United States v. Rahman, 189 F.3d 88, 111-114 (2d Cir. 1999).
[110] *Id.* 112-14.
[111] *Id.* at 113.
[112] *Id.* at 113-14.
[113] United States v. Augustin, 661 F.3d 1105, 1117 (11th Cir. 2011).
[114] *Id.*
[115] *See* Kawakita v. United States, 343 U.S. 717, 734 (1952).

element.[116] In addition, the extraterritorial effect of the Treason Clause has no bearing on prosecutions for traitorous conduct within the United States.

Based on these observations, the most prosecuted criminal laws to punish terrorist activity within the United States fall within the definition of treason and should implicate the rule against constructive treasons. However, there have only been a few instances where parties challenged these laws under this argument and in each instance, the court upheld the laws.

B. Modern Homegrown Terrorism

After the terrorist attacks on September 11, 2001, the United States faced grave threats at home and abroad from radical extremists, including the growth of ISIL. ISIL's rise to prominence led to unprecedented levels of recruiting and support throughout much of the globe.[117] ISIL was designated a FTO as an offshoot of Al Qaeda in Iraq in 2014.[118] Taking advantage of social media and encrypted messaging applications, ISIL spread its message and influence throughout much of the Western world.[119] By January 2016, thousands of foreigners and at least 200 Americans had either gone or attempted to go to Syria to help support ISIL's movement.[120] The ISIL-inspired attack on San Bernardino is a prime example of the danger that this group presents to the nation's security.[121] Homegrown terrorism inspired by the message ISIL promotes is one

---

[116] *Rahman*, 189 F.3d at 113.
[117] Naila Inayat & Kaci Racelma, *Islamic State Influence Spreads Beyond Iraq and Syria*, USA TODAY (Oct. 2, 2014), http://www.usatoday.com/story/news/world/2014/10/01/islamic-state-spread-pakistan-india-china-mali/16507043/.
[118] In the Matter of the Amendment of the Designation of al-Qa'ida in Iraq, 79 Fed. Reg. 27,972, 27,972 (May 15, 2014).
[119] Ray Sanchez, *ISIS Exploits Social Media to Make Inroads in U.S.*, CNN (June 5, 2015), http://www. cnn.com/2015/06/04/us/isis-social-media-recruits/.
[120] *Id.*; Payne, *supra* note 13.
[121] Paul D. Shinkman, *The Evolving Extremist Threat*, U.S. NEWS (Dec. 7, 2015), http://www.usnews.com/ news/articles/2015/12/07/san-bernardino-shooting-shows-evolving-isis-threat.

of the gravest threats to America's national security faced in this era.[122]

Two prime examples of the kinds of actions taken by homegrown terrorists are the cases of Christopher Cornell and Hanad Mustofe Musse. Throughout 2014, Christopher Cornell, a U.S. citizen of Green Township, Ohio, allegedly created a Twitter account using an alias and began posting statements and videos in support of ISIL calling for violent attacks in North America.[123] In August 2014, Cornell allegedly made contact with a confidential informant indicating he had been in contact with ISIL members overseas and that he wished to carry out attacks against the United States.[124] Through further conversations with the informant, Cornell expressed his desire to obtain weapons and build pipe bombs to carry out an attack against the U.S. Capitol Building in Washington, D.C.[125] On January 14, 2015, Cornell was arrested by federal officials after he had purchased two semi-automatic rifles and about 600 rounds of ammunition from an Ohio gun store.[126] The United States initially charged Cornell with attempting to kill a federal employee and possession of a firearm in furtherance of a violent crime.[127] However, a superseding indictment added an additional charge of attempting to provide material support to a terrorist organization in the form of personnel and services.[128]

Throughout 2014, Hanad Mustofe Musse, an American citizen living in Minneapolis, Minnesota joined a group of individuals who wished to travel overseas to join ISIL and discussed methods of obtaining transport.[129] Musse then used money from his federal financial aid account to purchase a bus ticket to New York City to meet with his co-conspirators to take a plane to Athens,

---

[122] *Id.*
[123] Criminal Complaint at 2-4, United States v. Cornell (S.D. Ohio filed Jan. 14, 2015) (No. 1:15-mj-00024).
[124] *Id.* at 3-5.
[125] *Id.* at 4-5.
[126] *Id.* at 5.
[127] Perry, *supra* note 2.
[128] Cornell Press Release, *supra* note 1.
[129] Musse Press Release, *supra* note 7.

Greece, from which they planned to travel to Syria.[130] This attempt failed when federal agents prevented Musse from boarding the plane at John F. Kennedy International Airport.[131] Following this failed attempt, Musse continued to make plans to travel to Syria and provided a passport photo to an informant in an attempt to obtain a false passport to use to travel to Syria through Mexico.[132] Musse was arrested and pleaded guilty to conspiring to provide material support to ISIL in September 2015.[133]

The Cornell and Musse cases provide a strong example of the type of threat homegrown terrorists pose. They also serve as useful case studies in how treason is the most appropriate method of prosecution for individuals who seek to betray the allegiance to the United States through terrorist actions.

III. APPLYING THE TREASON CLAUSE

As discussed above, many criminal statutes punish traitorous conduct under a different name with lesser penalties. Each of these criminal statutes possess the same elements as treason and most prosecutions under these statutes can also be prosecuted as treason, but without the procedural protection the Framers intended such prosecutions to provide.[134] The Musse and Cornell cases provide good examples of homegrown terrorist conduct in which prosecutors can successfully bring treason charges.

Hanad Musse ultimately pleaded guilty to conspiring to provide material support to a FTO in the form of personnel, including himself.[135] The actions Musse committed can be appropriately charged as treason in the form of adhering to the enemy, by providing them aid and comfort. Based on his attempted travels to Syria and information from his co-conspirators, Musse knew of ISIL's mission and location and he shared the same intent as

---

[130] *Id.*
[131] *Id.*
[132] *Id.*
[133] *Id.*
[134] *See, e.g.,* 18 U.S.C. § 2339B (2015); 18 U.S.C. § 2384 (1994).
[135] Musse Press Release, *supra* note 7.

the group. This shows that Musse adhered to an enemy of the United States, by sharing the same goal and intent to aid.[136] Additionally, providing personnel to an enemy provides aid and comfort in the form of stronger support and more soldiers on the battlefield.

There are several overt acts Musse committed, which provide the basis for a treason conviction, including meetings and discussions with co-conspirators, transfer of funds to purchase bus and plane tickets, his travel to New York City and attempt to fly to Greece, and his repeated attempts to obtain a false passport.[137] As long as testimony from at least two witnesses supports each of these overt acts, a treason conviction would likely be sustainable.

The United States charged Christopher Cornell with both attempting to kill federal employees and attempting to provide material support to a terrorist organization in the form of personnel and services.[138] A court could potentially try these actions as treason in a similar fashion to that of Musse. The statements Cornell allegedly made to the confidential informant showed his association with and support for ISIL and its goals.[139] Similar to Musse, this shows his adherence to an enemy of the United States. As discussed above, providing personnel and services to an enemy amounts to providing aid and comfort.[140] Cornell was allegedly planning to carry out an attack on the U.S. Capitol and his purchase of semi-automatic rifles was a substantial step in executing his plan.[141] The purchase of these weapons, along with the statements made to the confidential

[136] This section assumes the United States considers ISIL an "enemy", because the U.S. is actively engaged in military operations against them. *See, e.g.*, Letter from President Obama to the United States Congress, Authorization for the Use of United States Armed Forces in Connection with the Islamic State of Iraq and the Levant (Feb. 11, 2015), https://www.whitehouse.gov/the-press-office/2015/02/11/letter-president-authorization-use-united-states-armed-forces-connection.
[137] Musse Press Release, *supra* note 7.
[138] Cornell Press Release, *supra* note 1.
[139] Criminal Complaint at 3-4, United States v. Cornell (S.D. Ohio filed Jan. 14, 2015) (No. 1:15-mj-24).
[140] *See, e.g.*, *In re* Charge to Grand Jury, 30 F. Cas. 1034, 1035 (S.D.N.Y. 1861).
[141] Criminal Complaint at 4-5, United States v. Cornell (S.D. Ohio *filed* Jan. 14, 2015) (No. 1:15-mj-24).

informant are both overt acts which can support a treason conviction as long as testimony from at least two witnesses proves it.

The problem with these and similar cases, is that the defendants did not complete the crime, so aid and comfort was not actually provided to an enemy of the United States. As with most terrorism crimes, the primary goal of law enforcement is to prevent future attacks, rather than waiting for an attack to occur. Under the *Cramer* Court's interpretation of the Treason Clause, this goal would be impossible to fulfill under a treason prosecution, because aid and comfort cannot be given in these situations without either an attack being carried out (i.e. in the Cornell case), or a person leaving the jurisdiction of the United States (i.e. the Musse case). In order for treason to be a robust and feasible means for preventing terrorist attacks and punishing those who seek to commit them, the interpretation that aid and comfort must actually be given to support conviction must be overruled.

The proper interpretation of both the levying war and aid and comfort elements should include overt acts whose natural consequences amount to levying war or providing aid and comfort. For example, if a person has the intent to go overseas and join a terrorist organization to conduct attacks with them, and they carry out substantial steps towards that plan (i.e. purchasing a plane ticket and attempting to board), then the natural consequences of such an overt act would be to provide aid and comfort to an enemy of the United States. This would be in accordance with the understanding of the Treason Clause prior to *Cramer*. An act which "strengthens, or tends to strengthen" an enemy of the United States is the classic definition of an overt act which provides aid and comfort.[142] Included in "tends to strengthen" are actions whose natural effect is to strengthen an enemy.[143] The actions that both Musse and Cornell attempted, had they been able to carry out their plan, are actions that would have strengthened an enemy. Joining a terrorist organization overseas and carrying out an attack in the name of a terrorist organization have natural consequences, which strengthen the

[142] *See* U.S. v. Fricke, 259 F. 673, 676 (S.D.N.Y. 1919).
[143] *See id.*

message and support for these terrorist organizations. A natural consequences approach to the treason clause would allow law enforcement to prevent attacks by arresting and prosecuting suspected terrorists when their actions show both treasonous intent and have the effect of strengthening enemy terrorist organizations.

Note that preparation for a treason prosecution must begin in the investigatory stage. Because of the two-witness requirement, a prosecutor must support all overt acts with the testimony of two witnesses. This is important, especially during the investigation stage, because at least two individuals must witness every action amounting to treasonous conduct in order to make it to a jury in a treason trial. If only one individual witnesses an action, then it cannot be factored into the totality of the circumstances of whether the defendant's actions are treasonous. Law enforcement and prosecutors in terrorism cases must conduct their investigations with this procedural restriction in mind in order to overcome it and properly prosecute homegrown terrorist activities as treason.

IV. TREASON IS THE MOST APPROPRIATE CHARGE FOR HOMEGROWN TERRORIST CRIMES

"[T]here is no crime which can more excite and agitate the passions of men than treason . . . "[144] For this reason, treason prosecutions have been extremely rare and only done near times of war.[145] However, because of the changing nature of terrorist recruiting efforts and the rise of homegrown terrorist activity, the treason charge is once again becoming relevant in the current struggle against terrorism. Charging U.S. citizens who seek to commit these terrorist activities with treason provides positive societal benefits beyond typical law enforcement purposes of deterrence and punishment. Additionally, charging individuals with treason avoids constitutional issues with the current statutes under the rule against constructive treasons.

---

[144] *Ex parte* Bollman, 8 U.S. 75, 125 (1807).

[145] Lauren Prunty, *Terrorism as Treason: US Citizens and Domestic Terror*, JURIST (Sept. 11, 2011), http:// jurist.org/dateline/2011/09/lauren-prunty-domestic-terrorism-treason.php.

A. Treason Provides Many Positive Societal Benefits That Current Statutes Do Not Provide

The current statutory scheme treats defendants accused of supporting FTOs like ordinary criminals. This does not fully acknowledge the severity of the crime they have committed. As discussed above, U.S. citizens charged with seditious conspiracy and providing material support to terrorist organizations have also committed treason against the United States. Prosecuting these individuals with treason provides other benefits besides that of typical law enforcement purposes of deterrence and punishment.

Charging U.S. citizens accused of traitorous conduct with treason reaffirms a sense of allegiance and loyalty to the United States. All U.S. citizens and foreigners residing in the United States owe allegiance to the United States.[146] Prosecuting those who seek to betray this sense of allegiance for treason affirms the notion that "betrayal of our country will bring severe consequences."[147]

Because treason charges can reinforce societal identity and allegiance, treason prosecutions also show solidarity against enemies of the United States. The problem with this in the terrorism context would be that it could legitimize these organizations.[148] All previous treason trials have concerned state enemies. Considering non-state terrorist organizations as enemies of the United States could have the effect of giving these organizations legitimacy on the same level as state actors. However, this problem would be minimal in light of the fact that the United States is already engaged in armed conflict with many of these terrorist organizations, and they are treated similar to state actors in this regard. Additionally, labeling a terrorist

---

[146] *See* Kawakita v. United States, 343 U.S. 717, 734 (1952); Carlisle v. United States, 83 U.S. 147, 154 (1872).

[147] *See* Deputy Attorney General Paul McNulty, et al., U.S. Dept. of Justice, Transcript of Press Conference Announcing Indictment of U.S. Citizen for Treason and Material Support Charges for Providing Aid and Comfort to al Qaeda (Oct. 11, 2006), http://www.justice.gov/archive/dag/speeches/2006/dag_speech_061011.htm.

[148] *See* Kristen E. Eichensehr, *Treason in the Age of Terrorism: An Explanation and Evaluation of Treason's Return in Democratic States*, 42 VAND. J. TRANSNAT'L L. 1443, 1495-97 (2009).

organization an enemy of the United States does not change the nature of the conflict against it, but rather affirms the nation's mission to defeat it both abroad and domestically.

Another benefit of the treason charge is avoidance of the constitutional issues surrounding military detention and status of enemy combatants, at least when applied to U.S. citizens and individuals temporarily residing within the United States. Since the War on Terror began following 9/11, a major legal debate has been whether to deal with terrorism issues as a military or civilian matter.[149] Though treason charges would not work for many enemy combatants overseas, it would be an appropriate charge for U.S. citizens captured abroad. Charging these individuals with treason in a civilian court would have more constitutional legitimacy than trying them in military commissions because the crime of treason comes directly from the Constitution, rather than the tenacious authority for military tribunals garnered from *Ex parte Quirin*.[150]

Compared to the currently enforced statutes, treason offers prosecutors a broader range of potential punishment.[151] The maximum punishment for seditious conspiracy and material support are 20 years and 15 years in prison, respectively, while only authorizing longer punishment for material support if a death results.[152] Treason, on the other hand, provides a wide range of punishment ranging from a minimum five years to life of incarceration, as well as a large fine.[153] Treason can also be a capital offense.[154] This wide range of punishments allows prosecutors wider discretion to tailor their sentencing recommendations to fit the nature of the crime. As seen from an application of treason to the *Musse* and *Cornell* cases, treason cases can vary considerably in degree of severity and harm. Having such a broad range of potential

[149] *See, e.g.*, Hamdi v. Rumsfeld, 542 U.S. 507, 554 (2004) (Scalia, J., dissenting); *see also* Eichensehr, *supra* note 148, at 1492-94.
[150] *See Hamdi*, 542 U.S. at 519 (citing *Ex parte Quirin* as one authority authorizing detention of United States citizens as enemy combatants during hostilities); *see also* Eichensehr, *supra* note 148, at 1493-94.
[151] *Compare* 18 U.S.C. § 2381 (1994), *with* 18 U.S.C. §§ 2339B, 2384 (2015).
[152] 18 U.S.C. §§ 2384, 2339B.
[153] 18 U.S.C. § 2381.
[154] *Id.*

sentences gives prosecutors better ability to recommend a sentence, which fits the severity of the traitorous conduct, which the current statutes fail to recognize. A potential drawback to charging more individuals accused of terrorist activity with treason is that treason is a death penalty eligible offense.[155] However, principles of prosecutorial discretion solve this problem because a prosecutor seeking the death penalty for a treasonous offense which did not cause loss of life, will have to contend with current trends towards prohibiting the death penalty for crimes that do not result in death.[156]

Because they punish the same conduct and provide a lesser punishment, some might regard the current statutes as a pretext for treason. Charging with these lesser crimes sets these individuals free sooner than is reasonable and sends a signal that federal law enforcement cannot prove terrorism crimes.[157] Charging U.S. citizens accused of terrorism crimes with treason avoids this problem, because treason is the highest crime possible against the country, and it provides a wide range of potential punishments that can better fit the crimes people commit.

B. Current Statutes Present Strong Constitutional Concerns Under the Rule Against Constructive Treasons

Not only would treason prosecutions for homegrown terrorist activities provide strong societal and law enforcement benefits, they would also avoid constitutional concerns arising from the current statutes under the rule against constructive treasons. It follows that since the Constitution defines treason, and the Constitution only authorizes Congress to determine the punishment for the offense;[158] Congress may not proscribe the same offense under a different name with lesser procedural protections. This is the rule against constructive treasons and this is what Congress has done through these statutes.

---

[155] *Id.*

[156] *See* Eichensehr, *supra* note 148, at 1498-1503.

[157] *See* Daniel C. Richman & William J. Stuntz, *Al Capone's Revenge: An Essay on the Political Economy of Pretextual Prosecution*, 105 COLUM. L. REV. 583, 618-24 (2005) (discussing charging terrorist suspects with immigration violations).

[158] *See* U.S. CONST. art. III, § 3, cl. 1.

The seditious conspiracy and material support statutes both prohibit conduct, which is also triable under the Treason Clause. Because of this similarity, the statutes implicate the rule against constructive treasons and are at least unconstitutional as applied in many situations involving homegrown terrorism. Admittedly, some conspiracies may be triable under seditious conspiracy that may not amount to levying war under the Treason Clause, because of insufficient capability to use force against the United States, and because some designated terrorist organizations may not be appropriately labeled "enemies" of the United States. However, these situations would be rare because a court would likely consider any terrorist organization the United States is actively conducting military operations against an "enemy" of the United States, and prosecutors would theoretically not charge a suspect involved in a conspiracy until the conspiracy had ripened or come close to operational capability.

The Circuit Courts that have upheld these statutes against constructive treason challenges all distinguished them based on the absence of an allegiance element.[159] These courts failed to recognize that when applied to prosecutions against citizens or individuals residing within the United States, the allegiance element is established automatically and does not require a separate finding. Because of this misconception, these courts decided not to rule on whether Congress can remove procedural protections guaranteed by the Constitution by calling treason by a different name. Based on the history behind the Treason Clause, this amounts to creating a constructive treason and is unconstitutional. Prosecuting homegrown terrorists for treason would avoid this constitutional issue while also meeting the same law enforcement goals of preventing and deterring attack.

V. CONCLUSION

The Treason Clause of the Constitution mandates that treason shall consist only of levying war against the United States or

[159] *See* United States v. Augustin, 661 F.3d 1105, 1117 (11th Cir. 2011); United States v. Rahman, 189 F.3d 88, 111-14 (2d Cir. 1999); United States v. Rodriguez, 803 F.2d 318, 320 (7th Cir. 1986).

adhering to their enemies, giving them aid and comfort.[160] In spite of this, Congress passed criminal statutes that prohibit giving aid and comfort to terrorist enemies of the United States as well as statutes that prohibit conspiring to levy war or overthrow the government using force.[161] Both of these actions fall squarely within the definition of treason as expounded by the Framers, but prosecutions under these statutes fail to provide the two-witness procedural protections, which a prosecution for treason would require. For this reason, the charge of treason is the most suitable charge for prosecuting homegrown terrorists seeking to support terrorist organizations by both carrying out attacks on the homeland and traveling overseas to join them.

Treason cannot be a feasible charge used to prevent terrorist attacks without overruling the *Cramer* Court's interpretation that aid and comfort must actually be given to support a treason conviction. This interpretation does not follow lower court precedent regarding treason in the period before World War II and has limited lasting applicability. A more appropriate interpretation of this language is that the natural consequences of an action that amounts to levying war or giving aid and comfort to an enemy should be treated as treasonous. This solution provides law enforcement adequate means to prosecute terror suspects before they carry out attacks and provides substantial punishment for individuals seeking to betray this country.

The threat from homegrown terrorists to the security of the United States is immense and continuously growing. In order to both prevent attacks and provide a strong deterrent to this conduct, prosecutors should utilize the treason charge as a means for prosecuting and punishing individuals who seek to commit terrorist attacks against the United States. Prosecuting for treason rather than lesser statutes that cover the same conduct sends a proper signal, vindicating the societal sense of allegiance and solidarity against enemies of the United States while also avoiding constitutional issues presented by current statutes that punish the same conduct. Treason

[160] U.S. CONST. art. III, § 3, cl. 1.
[161] *See* 18 U.S.C. §§ 2339B, 2384 (1994, 2015).

is the most appropriate charge for the prosecution of homegrown terrorists seeking to travel overseas to join terrorist organizations or support them by carrying out attacks on U.S. soil.

COMMENT

HACKING FEDERAL CYBERSECURITY LEGISLATION: REFORMING LEGISLATION TO PROMOTE THE EFFECTIVE SECURITY OF FEDERAL INFORMATION SYSTEMS

Chelsea C. Smith*

In 2015, the U.S. Office of Personnel Management announced that it had experienced multiple cybersecurity incidents that resulted in the compromise of sensitive information for over 22 million individuals. These breaches represent the worst cyber intrusions in the history of the U.S. Federal Government. Cybersecurity is a growing national security concern, but the United States does not have a sufficient legislative framework to ensure the protection of federal information systems. While the Federal Information Security Modernization Act of 2014, which reformed the Federal Information Security Management Act of 2002, is intended to provide a framework for information security controls for federal agencies, it has been limited and ineffective. Congress must reform legislation to establish meaningful standards, to ensure methods of accountability to promote compliance, and to dedicate appropriate resources to safeguarding federal information systems. Without action, federal systems will remain at risk and become increasingly susceptible to cyber attacks similar—or worse—to the malicious attacks OPM recently faced.

* George Mason University School of Law, J.D. Candidate, May 2018.

"The United States is fighting a cyber war today, and we are losing."[1]

INTRODUCTION

Social Security numbers, dates and places of birth, health information, employment records, financial information, residency details, educational history, personal contacts, and even fingerprints; these are merely samples of the information that an adversary now

[1] Mike McConnell, *Mike McConnell on How to Win the Cyber-War We're Losing*, WASH. POST, Feb. 28. 2010, at B1 (Mike McConnell served as the Director of the National Security Agency from 1992 to 1996 and the Director of National Intelligence from 2007 to 2009).

holds due to a cyber attack on vulnerable U.S. government systems and networks.[2]

In June 2015, the U.S. Office of Personnel Management ("OPM") announced cybersecurity incidents on its systems that resulted in the compromise of sensitive, personally identifiable information ("PII") (e.g., Social Security number, date of birth) for over 22 million individuals.[3] These incidents also included the loss of "less sensitive," public information (e.g., names, phone numbers, and addresses) of countless others.[4] The stolen data represents "a treasure trove of information about everybody who has worked for, tried to work for, or works for the U.S. government."[5]

These breaches have collectively been described as the worst cyber intrusion in the history of the U.S. Federal Government.[6] As

---

[2] *See News Release: OPM Announces Steps to Protect Federal Workers and Others from Cyber Threats*, U.S. OFF. OF PERSONNEL MGMT. (July 9, 2015), https://www.opm.gov/news/ releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats [hereinafter *News Release: OPM Announces Steps*]; *News Release: OPM to Notify Employees of Cybersecurity Incident*, U.S. OFF. OF PERSONNEL MGMT. (June 4, 2015), https://www.opm.gov/ news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident [hereinafter *News Release: OPM to Notify Employees*].

[3] *See News Release: OPM Announces Steps*, *supra* note 2; *News Release: OPM to Notify Employees*, *supra* note 2.

[4] *See News Release: OPM Announces Steps*, *supra* note 2; *News Release: OPM to Notify Employees*, *supra* note 2. *See also* Sen. Ben Sasse, *Senator Sasse: The OPM Hack May Have Given China a Spy Recruiting Database*, WIRED (July 9, 2015, 5:36 PM), http://www. wired.com/2015/07/senator-sasse-washington-still-isnt-taking-opm-breach-seriously (addressing the types of contacts that individuals provide to OPM when applying for a background investigation).

[5] Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, WASH. POST (July 9, 2015), https://www.washingtonpost.com/blogs/ federal-eye/wp/2015/07/09/ hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say.

[6] *See, e.g.*, Jason Chaffetz, *The Breach We Could Have Avoided*, THE HILL (Sept. 30, 2015, 7:56 PM), http://thehill.com/special-reports/data-security-october-1-2015/ 255563-the-breach-we-could-have-avoided. *See also* Evan Perez & Shimon Prokupecz, *U.S. Data Hack May be 4 Times Larger than Government Originally Said*, CNN (June 23, 2015, 10:59 PM), http://www.cnn.com/2015/06/22/politics/opm-hack-18-milliion; Tom Risen, *Obama Considers Sanctions After Cyberattacks*, U.S. NEWS & WORLD REPORTS (June 15, 2015, 5:43 PM),

these incidents illustrate, cybersecurity is an area of increasing concern within the national security realm. According to the Director of National Intelligence ("DNI"), "[c]yber threats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of impact."[7] As such, there have been significant efforts and investments in building our ability to detect and respond to cyber threats from both domestic and foreign parties.

Despite these efforts, the United States currently lacks an effective cybersecurity legislative framework for the regulation of federal information systems,[8] and the federal functions associated with information security are disjointed and spread across government.[9] While some limited regulatory legislation exists, the government lacks an enforcement mechanism to ensure federal agency compliance with statutory cybersecurity requirements. As a result, government entities are increasingly susceptible to cyber attack, as evidenced by the recent OPM cyber breaches. Congress needs to take legislative action related to cybersecurity to establish a regulatory framework that includes measurable standards for federal agencies to implement. This must include enforcement mechanisms for compliance with established standards, processes to ensure agency accountability for protecting the government's information infrastructure, and added flexibility to government agencies to support recruiting individuals with the expertise to maintain effective information security programs.

This Comment explores cybersecurity legislation that targets the regulation of federal agencies, centering on the Federal Information Security Modernization Act of 2014 ("FISMA 2014"),

---

http://www. usnews.com/news/ articles/2015/06/15/obama-considers-sanctions-after-opm-breach.

[7] James R. Clapper, *Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community*, S. Armed Services Comm. 1 (Feb. 26, 2015).

[8] *See* JOHN ROLLINS & ANNA C. HENNING, CONG. RESEARCH SERV., R40427, COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE: LEGAL AUTHORITIES AND POLICY CONSIDERATIONS 4 (2009) ("Legislators and analysts have expressed concerns that the current statutory framework inadequately addresses modern cybersecurity threats.").

[9] *See* ERIC A. FISCHER, CONG. RESEARCH SERV., R43831, CYBERSECURITY ISSUES AND CHALLENGES: IN BRIEF 3 (2014).

which reformed the Federal Information Security Management Act of 2002 ("FISMA 2002") as the primary legislation enacted for regulating federal organizations. This Comment utilizes the recent cyber attacks on OPM as an illustrative example to evaluate this legislation's effectiveness in protecting federal systems and preventing future cyber intrusions from occurring.

Part I provides background on cybersecurity, as well as current and proposed legislation related to the protection of federal systems. Part II describes cybersecurity and the threats that the United States faces in cyberspace. This analysis includes a descriptive overview of cybersecurity, types of cyber threats, where the threats originate, and ways the United States can and has responded to these threats. Part III first discusses the current legislative framework that targets protection of federal systems against cyber attacks, analyzing the effectiveness of FISMA 2002 and its subsequent reform under FISMA 2014. This section next briefly explores the Federal Information Security Management Reform Act of 2015 ("FISMRA 2015"), which a bipartisan group of legislators proposed for enactment following the identification of the OPM cyber incidents. Lastly, to provide a comparison between legislative and executive branch responses, this section addresses Executive Orders to demonstrate how the executive branch has been involved in cybersecurity regulation. Finally, Part IV provides a recommendation for modifying current and proposed legislation to improve the protection of the federal information infrastructure to address the challenges this piece identifies.

I. BACKGROUND: CYBERSECURITY AND THE LAW

This section provides an overview of the term cybersecurity, as it applies to this Comment, particularly in its relation to national security. It concludes with a brief overview of current and pending legislation related to cybersecurity and the protection of federal systems. This section describes the need to take immediate legislative measures to improve our federal information infrastructure.

A. Cybersecurity and its Ties to National Security

Cybersecurity (sometimes referred to as information security) includes the efforts, activities, and processes associated with protecting digital information and critical information systems and infrastructures, including computers, networks, and programs, from unauthorized access.[10] A cyber attack occurs when one or more actors deliberately attempt to access and/or alter computer systems, networks, or information technology programs.[11]

Cybersecurity is becoming one of the largest national security concerns within the United States because cyber attacks present one of the most severe threats to the nation.[12] Recognizing the increased threat of cyber espionage and attack,[13] the White House identified the need to secure the nation's cyberspace as a critical component of its National Security Strategy.[14]

Despite agreement that protection of our nation's information systems is a critical priority, efforts to safeguard federal systems have been lacking.[15] Information stored on federal systems is often sensitive in nature (e.g., tax records containing private financial information, Social Security records, proprietary business information, defense and national security records), and

---

[10] *See* David G. Delaney, *Cybersecurity and the Administrative National Security State: Framing the Issues for Federal Legislation*, 40 J. LEGIS. 251, 251 (2013-2014).
[11] *See, e.g.*, Matthew F. Ferraro, *"Groundbreaking" or Broken? An Analysis of SEC Cybersecurity Disclosure Guidance, Its Effectiveness, and Implications*, 77 ALB. L. REV. 297, 307 (2013-2014) (describing "cyber attack" as the deliberate action to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information in these systems or networks).
[12] *See, e.g.*, 161 CONG. REC. S5456 (daily ed. July 22, 2015) (statement of Sen. Mark Warner); ROLLINS & HENNING, *supra* note 8, at 1 ("Cybersecurity has been called 'one of the most urgent national security problems facing the new administration.'").
[13] *See, e.g.*, Ferraro, *supra* note 11, at 309-10.
[14] THE WHITE HOUSE, NATIONAL SECURITY STRATEGY 1, 3 (2015), https://www.whitehouse.gov/sites/ default/files/docs/2015_national_security_ strategy_2.pdf.
[15] Robert Silvers, *Rethinking FISMA and Federal Information Security Policy*, 81 N.Y.U. L. REV. 1844, 1846 (2006) (identifying that "efforts to secure federal data have been marked by delay, inefficiency, and ineffectiveness").

unauthorized access can be devastating to the government.[16] However, there are limited regulations focused on ensuring cybersecurity of federal systems. And where regulation exists, federal agencies have been slow in satisfying the requirements for information security, and oversight and enforcement of these requirements is weak.[17]

B. Cybersecurity Legislation

The nation's cybersecurity concerns include the ability to protect federal systems and the critical information stored on these systems. In an effort to address these concerns, over the last fifteen years, Congress enacted some regulatory legislation designed to protect federal information systems.

Congress enacted FISMA 2002 following the time-limited Government Information Security Reform Act of 2000 ("GISRA"), in response to the government's ineffective security of federal systems and information.[18] FISMA 2002 had the intended purpose of "provid[ing] a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets."[19] Details in Part III describe how FISMA 2002 focused federal agency efforts on ensuring effective computer security, and protecting against unauthorized access to federal systems.[20] It accomplished this by requiring annual reports to the Office of Management and Budget

[16] *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-08-571T, INFORMATION SECURITY: PROGRESS REPORTED BUT WEAKNESSES AT FEDERAL AGENCIES PERSIST 3-4 (2008) [hereinafter GAO-08-571T]; Silvers, *supra* note 15, at 1845.
[17] *See, e.g.*, GAO-08-571T, *supra* note 16, at 3.
[18] *The Federal Information Security Management Act of 2002: Hearing on H.R. 3844 Before the Subcomm. on Gov't Efficiency, Fin. Mgmt and Intergovernmental Relations of the Comm. On Gov't Reform*, 107th Cong., 42 (2002) [hereinafter Hearing on H.R. 3844] (Rep. Thomas Davis stated, "I am not satisfied with our Federal Government's overall performance in securing our information infrastructure. The bottom line is, we are still too vulnerable.").
[19] Purposes, 44 U.S.C. § 3541 (2012). Information security refers to "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction." Definitions, 44 U.S.C. § 3542(b)(1) (2012).
[20] Hearing on H.R. 3844, *supra* note 18, at 40-41.

("OMB"), the development of information security standards by the National Institute of Standards and Technology ("NIST"), and the creation of an information security incident center.[21] FISMA 2002 also mandated federal agencies to establish a Chief Information Officer ("CIO") position tasked with protecting the agency's computer systems from unauthorized access and cyber attacks.[22]

However, agencies encountered several challenges that limited the ability to achieve the goals of FISMA 2002. For example, FISMA 2002 assigned multiple federal agencies responsible for implementing the law, and agencies were unable to keep up with the ever-increasing threat of cyber attack from criminals, terrorists, and foreign state actors.[23] Addressing these challenges, Congress enacted FISMA 2014 to update FISMA 2002. Congress intended for this update to clarify and codify the roles of OMB and the U.S. Department of Homeland Security ("DHS"). It provided OMB the authority to oversee and manage information security across federal agencies, and formally established DHS as the agency responsible for executing the operational aspects of federal cybersecurity through the monitoring of federal systems.[24] FISMA 2014 also adjusted the way the government managed federal data breaches, by increasing transparency and establishing uniformity in the process for reporting cyber incidents.[25]

Despite these legislative changes regulating the information security of federal systems, the federal information infrastructure remains vulnerable to cyber attacks, as evidenced by the recent OPM cybersecurity incidents. Following these breaches, FISMRA 2015 was proposed. FISMRA 2015 seeks to reform FISMA 2014, by allowing DHS to operate intrusion detection capabilities on all federal agencies within the "dot-gov" domain, directing DHS to conduct risk assessments of networks within this federal purview, and requiring

---

[21] *Id.*
[22] Federal Agency Responsibilities, 44 U.S.C. § 3544 (2012); *see also* ROLLINS & HENNING, *supra* note 8, at 9.
[23] S. REP. NO. 113-256, at 2 (2014).
[24] *Id.* at 3-4.
[25] *Id.* at 7-8.

regular reports from OMB to Congress on the execution of their enforcement authorities under the statute.[26]

While FISMRA 2015 addressed some of the weaknesses of existing legislation, neither the proposal nor current law establishes strong cybersecurity standards and enforcement mechanisms under which federal agencies must comply. The current cybersecurity legislative framework is not working, and the nation's federal systems remain vulnerable to attack.[27] Until federal agencies are held accountable to strong standards for information security management, it is likely government agencies will remain susceptible to cyber attack.

II. CYBERSECURITY: THREATS AND RESPONSES

This section provides a detailed analysis of ongoing cybersecurity threats that the United States faces. This analysis includes a descriptive overview of cybersecurity, the types of existing cybercrimes and threats, who the primary threats are, and ways the United States can respond to these threats. This section sets the stage for the following section's discussion of the legislative actions that the United States implemented to protect federal systems from cyber threats.

A. The Threat of Cybercrime

Cyberspace, a necessary element of our economy and national security, serves as "the control system of our country" as it allows the United States' critical infrastructure to operate.[28] Countless

---

[26] 161 CONG. REC. S5456 (daily ed. July 22, 2015) (statement of Sen. Collins).
[27] Gus P. Coldebella & Brian M. White, *Foundational Questions Regarding the Federal Role in Cybersecurity*, 4 J. NAT'L SECURITY L. & POL'Y 233, 236 (2010).
[28] Melanie J. Teplinsky, *Fiddling on the Roof: Recent Developments in Cyber Security*, 2 AM. U. BUS. L. REV. 225, 233 (2012-2013) (quoting the DHS 2003 National Security Strategy to Secure Cyberspace). "Critical infrastructure" in this context refers to the "systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on national security." U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-714, FEDERAL INFORMATION SECURITY: AGENCIES NEED TO CORRECT WEAKNESSES AND FULLY IMPLEMENT SECURITY PROGRAMS 1 n.1 (2015) [hereinafter GAO-15-714].

interconnected computers, servers, and cables comprise cyberspace.[29] "Cyberspace affects every aspect of daily life."[30] However, the growth of technology, computing, and networking led to advances in crime within this cyberspace.[31] Crime in cyberspace is unique because the use of computers to perpetrate a crime is often less expensive, the internet makes it easier for criminals to communicate, and the activities are frequently undetected.[32] Cybercrime ranges from unauthorized access to computer programs, to disruption—and even destruction—of these files or programs, to actual theft of information and/or identities.[33] Cybercrime also includes cyber terrorism, which consists of any criminal or terrorist attack conducted in cyberspace that results in violence or destruction of its target and has the purpose of inciting terror and/or coercing a government.[34] Thus, securing the components of our nation's cyberspace is essential to our national security.[35]

Simply put, cybersecurity is the defense against cyber attacks and cybercrime.[36] Cyber attacks are occurring with increasing frequency, and, as such, have become a principal concern to national and homeland security communities.[37] The ability to destroy or impair virtual systems and assets that are vital to the U.S. national security could have a "debilitating impact on security, national economic security, national public health and safety, or any

[29] Teplinsky, *supra* note 28.
[30] Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 43 VAND. J. TRANSNAT'L L. 57, 73 (2010).
[31] *See, e.g.*, Eric G. Orlinsky, *Cyber Security: A Legal Perspective*, MD. B. J. 33, 34 (2014) ("The threat of a cyber attack and the extent of potential danger to an organization continues to grow with daily technological innovations."); Teplinsky, *supra* note 28.
[32] *See* Gable, *supra* note 30, at 60; Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1006-08 (2001).
[33] *See, e.g.*, Katyal, *supra* note 32, at 1013.
[34] Gable, *supra* note 30, at 62-63.
[35] Teplinsky, *supra* note 28.
[36] *See* Delaney, *supra* note 10; Stephen Dycus, *Congress's Role in Cyber Warfare*, 4 J. NAT'L SECURITY L. & POL'Y 155, 162 (2010); Gable, *supra* note 30, at 62-63.
[37] *See* Gable, *supra* note 30, at 60 (2010); ROLLINS & HENNING, *supra* note 8, at 2-3.

combination of those matters."[38] Admiral Michael Mullen, the former Chairman of the Joint Chiefs of Staff, described cyber threats as one of "two existential threats to the United States," with the other being nuclear proliferation.[39] A sophisticated cyber attack, similar to a nuclear attack, would likely come without clear warning and, because of a lack of a reliable and effective defense mechanism, would cause extensive, long lasting, and indiscriminate direct and indirect damage.[40]

Cyber war is becoming a reality,[41] and the United States is not prepared to defend against a sophisticated attack.[42] Actors engage in cyber terrorism or espionage where they use cyberspace to gather intelligence and information critical to national and economic security.[43] The U.S. information infrastructure serves as a constant target for cyber attack.[44] For example, on any given day, the U.S. Department of Defense experiences millions of attempted cyber attacks.[45] Over the last several years, cyber attackers have successfully accessed and compromised sensitive government and military information. For instance, over a two-year period, hackers obtained confidential files regarding the military's fighter aircraft from the U.S. Air Force's air traffic control systems.[46] These cyber attacks will

[38] ROLLINS & HENNING, *supra* note 8, at 2-3; *see also* Gable, *supra* note 30, at 74 ("Without ever having to build a bomb or sacrifice themselves, cyberterrorists can bring down the critical infrastructure of an entire state, disrupt the global economy, and instill fear and chaos among billions of people.").
[39] Ferraro, *supra* note 11, at 309.
[40] Dycus, *supra* note 36, at 163.
[41] Peter M. Shane, *Cybersecurity: Toward a Meaningful Policy Framework*, 90 TEX. L. REV. 87, 89 (2012).
[42] John S. Fredland, *Building a Better Cybersecurity Act: Empowering the Executive Branch Against Cybersecurity Emergencies*, 206 MIL. L. REV. 1, 4 (2010) (Mike McConnell, former Director of National Intelligence, claimed that U.S. adversaries have the ability to bring down a power grid through cyberattack and the "United States is not prepared for such an attack.").
[43] ROLLINS & HENNING, *supra* note 8, at 1.
[44] *See* Fredland, *supra* note 42, at 3; *see also* Mike Mount, *Hackers Stole Data on Pentagon's Newest Fighter Jet*, CNN (Apr. 21, 2009), http://edition.cnn.com/2009/US/04/21/pentagon.hacked (addressing an increase in attacks on U.S. military and government networks).
[45] *See, e.g.*, Fredland, *supra* note 42, at 3 ("On a single day in 2008, the Pentagon experienced six million attacks from would-be cyberintruders.").
[46] Mount, *supra* note 44.

only increase in sophistication.[47] "As cyberspace evolves, it is increasingly likely that threat actors can remotely cause kinetic attacks, disrupt vital national systems, or diminish government response capabilities."[48] Some senior government officials claim that the cyber attacks on the OPM systems and networks, and the resulting theft of data, should be called an act of war that requires retaliatory action.[49]

Protecting our vulnerabilities now plays a critical role in our national security strategy.[50] "Protecting networks, computers, programs, and data—and the critical infrastructures on which they rely—from attack, damage, or unauthorized access could hardly be more important."[51] The White House recently identified a focus of "fortifying our critical infrastructures against all hazards, especially cyber espionage and attack" in the U.S. National Security Strategy.[52] President Obama separately identified cyber attacks as "one of the most serious economic and national security challenges" facing our nation.[53] As cybercrime continues to increase in volume and degree of sophistication, it is likely the federal government will remain focused on strategically deterring against these cyber attacks and protecting its federal systems.

B. Sources of Cyber Threats

As cyberspace continues to grow, the type of crime and actors involved in cybercrime continues to evolve as well.[54] Cyber threats may come from a range of actors including foreign nation

---

[47] Shane, *supra* note 41.
[48] Delaney, *supra* note 10, at 257.
[49] Tom Leithauser, *OPM Cyber Attack was 'Act of War,' U.S. Should Retaliate, McCain Says*, CYBERSECURITY POL'Y REP. (2015).
[50] *See* Teplinsky, *supra* note 28, at 232 ("Our shared digital infrastructure is vulnerable to a wide-range of cyberthreats that are understood to pose some of the most serious economic and national security challenges of the 21st century.").
[51] Shane, *supra* note 41, at 87.
[52] THE WHITE HOUSE, *supra* note 14, at 3.
[53] Barack Obama, *Taking the Cyberattack Threat Seriously*, WALL ST. J. (July 19, 2012, 7:15 PM), http://www.wsj.com/articles/SB10000872396390444330904577535492693 044650.
[54] *See* Clapper, *supra* note 7, at 1.

states with sophisticated programs, nations with lesser technological capabilities but potentially a more hostile intent, criminals motivated for profit, and ideological extremists.[55] Thus, cybercrime may range from phishing attempts on individual citizens for financial gain to "advanced persistent threats," which are highly targeted malware attacks against government and military networks.[56]

Foreign actors have had increased success in recent years in obtaining access to critical infrastructure systems of the United States, but distinguishing actors has become difficult as coordination among foreign nation states expands and the skills and tools used to commit cybercrime develop.[57] According to a 2011 National Counterintelligence Executive Report, Chinese actors are the "the world's most active and persistent perpetrators of [cyber] economic espionage."[58] Similarly, Russia is establishing a cyber command that will conduct offensive cyber activities, such as inserting malware into enemy systems.[59] Other foreign cyber threats include Iran, North Korea, and various terrorist groups.[60] While the federal government and the Obama Administration have not attributed responsibility for the cyber intrusions on the OPM systems, unofficial sources have linked these attacks to China,[61] and this is not the first time officials have suspected China suspected of targeting OPM databases.[62]

---

[55] *Id.*; *see also* GAO-08-571T, *supra* note 16, at 5 (providing a list of sources of cyber threats prepared by the Federal Bureau of Investigation).
[56] *See* Teplinsky, *supra* note 28, at 256-57; *see also* GAO-15-714, *supra* note 28, at 1 ("[A]dvanced persistent threats—where an adversary that possesses sophisticated levels of expertise and significant resources can attack using multiple means such as cyber, physical, or deception to achieve its objectives—pose increasing risks.").
[57] Clapper, *supra* note 7, at 2.
[58] Teplinsky, *supra* note 28, at 260.
[59] Clapper, *supra* note 7, at 2.
[60] *Id.*
[61] *See* Ellen Nakashima, *Chinese Breach Data of Four Million Federal Workers*, WASH. POST (June 4, 2015), https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/ 889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html.
[62] Michael S. Schmidt, et al., *Chinese Hackers Pursue Key Data on U.S. Workers*, N.Y. TIMES (July 9, 2014), http://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html (discussing that, in a previous cyber beach of OPM's systems, the Chinese were accused of targeting employee files for

C. Responding to Cyber Threats and Preventing Cyber Attacks

Identifying the actor involved in a cyber attack can aid in determining the United States response following the attack.[63] For example, if the government determines financial gain or commercial purposes motivated an individual or group of cyber-attackers to seek out data, law enforcement may use traditional criminal justice tools for punishment.[64] However, if the United States is able to identify a foreign nation state as the perpetrator, it is unlikely that the United States will press criminal charges; rather, the response will likely include counterintelligence or military efforts.[65]

The last few Presidential Administrations also attempted to respond to the increase in cyber attacks in various ways.[66] President Clinton established the Critical Infrastructure Protection and the Presidential Information Technology Advisory Council.[67] President George W. Bush created the DHS and tasked the agency with cybersecurity,[68] and he established the Comprehensive National Cybersecurity Initiative to create a defense against network intrusion and strengthen the national cybersecurity environment.[69] President Obama appointed the first Federal CIO to identify and promote efficiencies related to information technology and cybersecurity.[70] Additionally, the Obama Administration released the International Strategy for Cyberspace to promote the flow of information on the internet while ensuring the security of data.[71]

---

those that had applied for Top Secret security clearances).

[63] KRISTIN FINKLEA ET AL., CONG. RESEARCH SERV., IN10287, CYBER INTRUSION ON U.S. OFFICE OF PERSONNEL MANAGEMENT 2 (June 5, 2015).

[64] *Id.* at 2-3.

[65] *Id.*

[66] Delaney, *supra* note 10, at 253.

[67] Gable, *supra* note 30, at 75.

[68] *See* Exec. Order No. 13,228, 66 Fed. Reg. 51,812 (Oct. 8, 2001) (establishing the Office of Homeland Security and charging this office with the protection of information systems); Homeland Security Act of 2002, Pub. L. No. 107-296, §§ 221-25, 116 Stat. 2135, 2155-59 (2002).

[69] Gable, *supra* note 30, at 75-76.

[70] THE WHITE HOUSE: TECHNOLOGY, https://www.whitehouse.gov/issues/technology (last visited Dec. 28, 2015).

[71] *Id.*

In addition to these executive branch responses, an effective legislative framework is a necessary element to ensuring the government can protect U.S. systems and networks from cyber threats.[72] Within the legislative branch, there has been a focus on increasing transparency by sharing information related to cyber attacks, particularly within the private sector, as barriers to information sharing are considered a limitation to effective cybersecurity.[73] For example, the 114th Congress introduced at least three bills that related to the sharing of information among private entities to protect information systems from unauthorized access.[74] Despite these recent efforts, Congress took little action. Currently, an effective framework of legislation for cybersecurity and the protection of federal systems and information infrastructure does not exist.[75]

The government must implement offensive and deterrent strategies to prevent cyber attacks from occurring. "What we need is a long-term, intelligence-driven strategy for safeguarding sensitive, personal information and for deterring future attacks."[76] To do this, Congress needs to reform cybersecurity legislation to develop meaningful standards, provide a means of accountability, and ensure appropriate resources are dedicated to safeguarding federal information systems.

III. CYBERSECURITY LEGISLATION: THE EVOLUTION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT

This section provides an overview of the current legislative framework that targets the protection of federal systems from cyber attacks, as well as the recent proposals to reform this legislation. This includes a discussion of the legislative branch's role in cybersecurity,

---

[72] *See* Dycus, *supra* note 36, at 155.

[73] ERIC A. FISCHER, CONG. RESEARCH SERV., R44069, CYBERSECURITY AND INFORMATION SHARING: COMPARISON OF H.R. 1560 (PCNA AND NCPAA) AND S. 754 (CISA) 1 (2015); Teplinsky, *supra* note 28, at 277 ("More recently, Congress and federal regulators have adopted a number of legislative and regulatory measures to improve transparency with respect to cyber incidents.").

[74] FISCHER, *supra* note 73.

[75] Delaney, *supra* note 10, at 276.

[76] Sasse, *supra* note 4.

an in-depth analysis of FISMA 2002, as well as its reform through FISMA 2014, including its purpose, structure, and criticisms of it. This section then reviews FISMRA 2015 and compares this proposed legislation with existing legislation to identify how it would modify the regulatory framework if the legislature enacted it. For comparison, this section also briefly explores how the executive branch has been involved in responding to cyber threats.

A. Role of the Legislative Branch in Cybersecurity

Congress is responsible for developing legislation to protect against, and respond to, cyber threats, particularly in the face of a potential cyber war. "If Congress is to be faithful to the Framers' vision of its role in the nation's defense, it must tighten its grip and play a significant part in the development of policies for war on a digital battlefield. It also must enact rules to help ensure that these policies are carried out."[77]

Cybersecurity legislation has predominantly focused on the protection of private entities, as the private sector owns and operates the majority of the United States critical information infrastructure.[78] Legislation in this area targeted information sharing between private corporations and the federal government, including the disclosure of security breach information.[79] Specifically, the federal government, and the majority of states enacted data breach notification laws, under which private corporations and public entities must disclose

[77] Dycus, *supra* note 36, at 155.
[78] Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1506 (2013) ("America's critical infrastructure, approximately 85% of which is owned by private firms, already faces constant intrusions.").
[79] *See id.*

data breaches that involve the compromise of sensitive information and PII.[80]

However, limited cybersecurity legislation and regulation addresses federal cybersecurity requirements or focuses on the protection of the federal information infrastructure.

> Part of our cybersecurity problem is institutional—we do not have organizations and practices in place to provide anything like efficient and effective governance in the cybersecurity area. But another huge part is regulatory. We simply do not have in place a framework of laws and regulations, 'smart' or otherwise, that adequately incentivizes the parties with the greatest capacity to improve our security to do so.[81]

Further, cyber attacks on government information infrastructures are increasing in frequency and sophistication, and a successful attack could be devastating.[82] Despite this grave call for action, there has been a great degree of inaction by Congress.[83] FISMA 2002, and subsequent reforms, serve as the only significant framework to ensure the information security of federal systems.[84]

---

[80] Alabama, New Mexico, and South Dakota remain the only states without security breach notification laws. *See Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last updated Oct. 22, 2015) (indicating that as of October 2015, 47 states, the District of Columbia, Puerto Rico, Guam, and the Virgin Islands have enacted data breach notification laws); *see also* Notification in the Case of Breach, 42 U.S.C. § 17932 (2012) (federal data breach notification law).

[81] Shane, *supra* note 41, at 95.

[82] ROLLINS & HENNING, *supra* note 8, at 2 ("Of paramount concern to the national and homeland security communities is the threat of a cyber related attack against the nation's critical government infrastructures . . . so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters.").

[83] *See, e.g.*, FISCHER, *supra* note 9, at 3 ("However, until the end of the 113th Congress, no bills on cybersecurity had been enacted since the Federal Information Security Management Act (FISMA) in 2002.").

[84] Delaney, *supra* note 10, at 277.

B. Federal Information Security Management Act of 2002

1. Overview of FISMA 2002

Congress enacted FISMA 2002 as Title III of the E–Government Act of 2002[85] in response to growing economic and national security concerns, and interests related to information security in the United States.[86] FISMA 2002 codified many aspects of the expiring GISRA,[87] and Congress intended FISMA 2002 to serve as legislative guidance to federal agencies in the development, promulgation, and compliance with management controls for information systems.[88] FISMA 2002 strengthened the requirements established under GISRA through the additional requirement for annual assessments of the effectiveness of information security systems, and the implementation of information security standards.[89] FISMA 2002 established mandatory minimum information security standards for all agencies; it required annual reports to OMB and the Comptroller General, exempting national security and intelligence related systems; and it required the establishment of a federal information security incident center, the United States Computer Emergency Readiness Team.[90] FISMA 2002 was supposed to serve as a comprehensive framework for ensuring effective security controls of federal information systems through various risk management activities.[91]

---

[85] E-Government Act of 2002, Pub. L. No. 107-347 (2003).
[86] *FISMA: Detailed Overview*, NAT'L INST. OF STANDARDS AND TECH., http://csrc.nist.gov/groups/SMA/fisma/ overview.html (last updated Apr. 1, 2014).
[87] PATRICK D. HOWARD, FISMA PRINCIPLES AND BEST PRACTICES: BEYOND COMPLIANCE 7 (2011) ("GISRA required each department or agency head to ensure that information security was provided throughout the life cycle for all agency information systems, and to ensure that agency officials assessed the effectiveness of the information security program, including the testing of information security controls.").
[88] Hearing on H.R. 3844, *supra* note 18, at 43 (statements by Rep. Thorner).
[89] HOWARD, *supra* note 87, at 8.
[90] Hearing on H.R. 3844, *supra* note 18, at 43 (statements by Rep. Thorner).
[91] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-137, INFORMATION SECURITY: WEAKNESSES CONTINUE AMID NEW FEDERAL EFFORTS TO IMPLEMENT REQUIREMENTS 2 (2011) [hereinafter GAO-12-137].

FISMA 2002 mandated that federal agencies develop information security strategies to protect their information systems by conducting assessments to identify vulnerabilities to attack, determining the magnitude of the potential harm that would result from cyber attack, and implementing appropriate safeguards to prevent such attacks.[92] Specifically, FISMA 2002 required each agency to "develop, document, and implement an agency wide information security program . . . to provide information security for the information and information systems that support the operations and assets of the agency."[93] FISMA 2002 placed these responsibilities on federal agencies with the presumption that agency officials (namely, CIOs) had the capability to understand risks and other factors related to information security that adversely affected their mission.[94]

2. Distribution of Responsibilities under FISMA 2002

FISMA 2002 assigned specific responsibilities to OMB, NIST, and federal agencies in its attempt to strengthen federal information technology systems. To ensure compliance with the statute, FISMA 2002 identified OMB as having oversight authority over agency actions, the development of information security programs, and the coordination with NIST in the development of information security standards and guidelines.[95] OMB's duties included reviewing agency plans for implementation of the FISMA 2002 requirements, receiving periodic updates from agencies on the status of their compliance, and submitting annual reports to Congress.[96] OMB was also responsible for developing policies and guidelines on information security, and providing instructions to federal agencies for preparing annual reports.[97] Under FISMA 2002, OMB had the power to enforce requirements through a variety of

[92] *See* Delaney, *supra* note 10, at 261; *see also* Silvers, *supra* note 15, at 1848.
[93] Federal Agency Responsibilities: Agency Program, 44 U.S.C. § 3544(b) (2006) (repealed 2014).
[94] *FISMA: Detailed Overview*, *supra* note 86.
[95] Authority and Functions of the Director, 44 U.S.C. § 3543(a) (2006) (repealed 2014).
[96] 44 U.S.C. § 3543(a)(8)(B)-(C) (repealed 2014); *see also* Silvers, *supra* note 15, at 1848-49.
[97] *See* GAO-08-571T, *supra* note 16, at 7.

sanctions and tools, including recommending a decrease in information resources or appropriations for agencies not complying with the requirements.[98] OMB's efforts to date primarily related to issuing guidance to agencies for reporting on a variety of metrics and measuring agency performance against these metrics, which are designed to evaluate agency compliance with FISMA 2002.[99]

FISMA 2002 tasked NIST with developing information security standards and guidelines for use by federal agencies.[100] This includes establishment of information system categories and the minimum requirements for federal information and information systems. As such, NIST established a "risk management framework" to consolidate the security standards and guidelines that FISMA 2002 required for agency use in their development of an information security program and risk management.[101] While this framework does not provide a "one-size-fits-all" approach to cybersecurity, it provides a broad, flexible, cost effective method for agencies to use in managing their cybersecurity risk.[102] However, use of the framework is not mandatory, nor enforced.[103]

Federal agencies are responsible for complying with FISMA 2002 and related policies, procedures, and guidelines and ensuring the overall agency strategic planning process incorporates information security management.[104] More specifically, each agency must maintain an information security program that is commensurate with its risk profile and the magnitude of harm that could result from unauthorized access to that agency's information

[98] Performance-based and Results-based Management: Enforcement of Accountability—Specific Actions, 40 U.S.C. § 11303(b)(5)(B) (2002); *see also* Silvers, *supra* note 15, at 1849.
[99] *See* GAO-15-714, *supra* note 28, at 6; OFFICE OF MGMT & BUDGET, EXEC. OFFICE OF THE PRESIDENT, ANNUAL REPORT TO CONGRESS: FEDERAL INFORMATION SECURITY MANAGEMENT ACT 9 (Feb. 27, 2015) [hereinafter OMB FY14 FISMA Report].
[100] 44 U.S.C. § 3543(a)(3) (2006) (repealed 2014).
[101] *FISMA: Detailed Overview*, *supra* note 86.
[102] Orlinsky, *supra* note 31, at 37.
[103] *Id.*
[104] 44 U.S.C. § 3544 (2006) (repealed 2014); *see also* Howard, *supra* note 87, at 10.

systems.[105] Therefore, each agency must conduct regular assessments of the risk posed to their information security programs, ensure risk-based policies and procedures are in place, establish plans for ensuring adequate information security, provide training for agency personnel on the appropriate use of information systems, and establish a process for identifying and addressing deficiencies to information systems.[106]

Each agency must also establish a CIO and a senior agency information security officer, who most agencies have designated as the Chief Information Security Officer ("CISO"), and agency heads must delegate to these individuals the necessary authority to ensure compliance under FISMA 2002.[107] The CIO and CISO's responsibilities include the development and maintenance of agency information security programs and policies, training of personnel in this functional area, and administration of advice and guidance to senior agency officials related to information security.[108]

In 2010, OMB gave DHS primary responsibility for the operational aspects of federal cybersecurity covered by FISMA 2002,[109] and in 2013, OMB assigned DHS the added responsibility of monitoring federal information systems with the intent of improving the government's ability to more immediately identify emerging cyber threats.[110] DHS must work with each agency to establish an information security continuous monitoring program.[111] OMB requires that these programs be designed to maintain DHS and

---

[105] 44 U.S.C. § 3544. *See also* GAO-08-571T, *supra* note 16, at 6; OMB FY14 FISMA Report, *supra* note 99, at 9.
[106] *See* GAO-08-571T, *supra* note 16, at 6-7.
[107] 44 U.S.C. § 3544(a)(3) (2006) (repealed 2014); *see also* HOWARD, *supra* note 87, at 10.
[108] HOWARD, *supra* note 87, at 11.
[109] OFFICE OF MGMT & BUDGET, EXEC. OFFICE OF THE PRESIDENT, OMB M-10-28, CLARIFYING CYBERSECURITY RESPONSIBILITIES AND ACTIVITIES OF THE EXECUTIVE OFFICE OF THE PRESIDENT AND THE DEPARTMENT OF HOMELAND SECURITY 1 (2010) [hereinafter OMB M-10-28].
[110] OFFICE OF MGMT & BUDGET, EXEC. OFFICE OF THE PRESIDENT, OMB M-14-03, ENHANCING THE SECURITY OF FEDERAL INFORMATION AND INFORMATION SYSTEMS 2 (2013) [hereinafter OMB M-14-03].
[111] *Id.* at 4.

agency awareness of information security, vulnerabilities, and risks, providing the government with the ability to respond in real-time to emerging cyber threats.[112] Following this shift in responsibilities to DHS, DHS began issuing guidance on the information security requirements and metrics for agencies to report on annually.[113]

3. Required Assessments and Reports Under FISMA 2002

FISMA 2002 required government agencies to provide an annual report to OMB, several congressional committees, and the Comptroller General.[114] This report described the effectiveness and adequacy of agency information security programs and policies, including compliance with the requirements established under FISMA 2002.[115] OMB, in turn, provided an annual report to Congress summarizing the independent assessments of agency information security programs (described below), evaluating agency compliance with the standards established by NIST, and identifying significant agency deficiencies in information security practices.[116] In addition to the annual reports, FISMA 2002 requires agencies to include information on security programs and standards in annual budget reports, program performance reports, financial management systems, and information technology management systems.[117]

In September 2009, OMB established a task force to review agency compliance with FISMA 2002, and develop metrics for agency reporting related to information security performance in an effort to advance the security posture of federal agencies.[118] As a result of this task force, OMB implemented a three-tiered approach to reporting under FISMA 2002, which included: data feeds directly from approved security management tools, government-wide

[112] *Id.* at 2.
[113] GAO-15-714, *supra* note 28, at 8.
[114] 44 U.S.C. § 3544(c) (2006); *see also* HOWARD, *supra* note 87, at 29.
[115] 44 U.S.C. § 3544(c); *see also* HOWARD, *supra* note 87, at 15.
[116] HOWARD, *supra* note 87, at 29.
[117] *Id.* at 16.
[118] OFFICE OF MGMT & BUDGET, EXEC. OFFICE OF THE PRESIDENT, OMB M-10-15, FY 2010 REPORTING INSTRUCTIONS FOR THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT AND AGENCY PRIVACY MANAGEMENT 1 (2010) [hereinafter OMB M-10-15].

benchmarking based on agency responses to questions related to its security posture, and agency-specific interviews conducted by a team of government security specialists to identify specific threats based on unique missions.[119] The three-tiered approach in agency reporting aimed at "implementing solutions that actually improve security," rather than a "culture of paperwork reports."[120] OMB maintained responsibility for submitting the annual FISMA report to Congress and made DHS responsible for overseeing agency compliance with FISMA 2002 and agency implementation of, and reporting on, cybersecurity policies and guidance.[121]

FISMA 2002 also mandated that each agency, through its Inspector General ("IG") or independent external auditors, conduct an annual independent evaluation of agency information security programs to determine the effectiveness of these programs.[122] Specifically, the IGs evaluate agency compliance with the statute, measure the effectiveness of information security programs through assessments of information security policies and practices, and identify vulnerabilities to agency information security programs.[123] Under FISMA 2002, agencies submit these evaluations annually to OMB.[124]

C. Federal Information Security Modernization Act of 2014

In December 2014, Congress decided to reform FISMA 2002 through the enactment of FISMA 2014 with the goal of improving federal cybersecurity.[125] FISMA 2014 maintained the same purpose as FISMA 2002, which was to provide a "comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets"

---

[119] *Id.* at 2-3.
[120] *Id.* at 3.
[121] OMB M-10-28, *supra* note 109, at 1-2.
[122] GAO-08-571T, *supra* note 16, at 8.
[123] 44 U.S.C. § 3545 (2006) (repealed 2014); HOWARD, *supra* note 87, at 16-17.
[124] GAO-08-571T, *supra* note 16, at 8.
[125] The Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283 (2014) (amending chapter 25 of Title 44, United States Code, and superseding the very similar Federal Information Security Management Act of 2002).

through government-wide management and oversight of information security risks and programs.[126] Congress intended FISMA 2014 to enhance and modernize the legislative framework for federal information security by clarifying and delegating responsibilities to OMB, DHS, NIST, agency heads, agency CIOs, agency CISOs, and agency IGs.[127]

FISMA 2014 updated FISMA 2002 specifically by clarifying OMB's oversight authority, including the authority to develop and oversee the implementation of information security policies; codifying DHS' authority to administer information security policies and provide technical assistance to federal agencies in the implementation of FISMA requirements; and simplifying reporting requirements to eliminate inefficient and wasteful reporting.[128] FISMA 2014 also reinforced FISMA 2002's requirement that agency heads provide information security programs and protections commensurate with their agency's risk profile.[129]

FISMA 2014 included a new section defining federal agency responsibilities, reestablishing that agencies are to implement agency-wide information security programs, establish a CIO position, report agency-specific cybersecurity incidents to Congress, and provide annual reports on the progress of implementing an information security program under FISMA 2014.[130] FISMA 2014 modified reporting requirements, mandating that agencies use automated tools and report more information related to cyber threats, security incidents, and compliance with FISMA 2014's

[126] 44 U.S.C. § 3541 (2012).
[127] *Is the OPM Data Breach the Tip of the Iceberg?*: *Hearing Before the Subcomm. On Research & Tech. and Oversight of the Comm. On Sci., Space, and Tech.,* 114th Cong. 4 (July 8, 2015).
[128] *See Federal Information Security Modernization Act (FISMA)*, U.S. DEPT. OF HOMELAND SECURITY, http://www.dhs.gov/fisma (last visited Oct. 16, 2015); S. REP. NO. 113-256, at 9-10 (2014).
[129] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-758T, INFORMATION SECURITY: CYBER THREATS AND DATA BREACHES ILLUSTRATE NEED FOR STRONGER CONTROLS ACROSS FEDERAL AGENCIES 3 (2015) [hereinafter GAO-15-758T].
[130] S. REP. NO. 113-256, at 10 (2014).

security requirements.[131] Additionally, FISMA 2014 required that the annual independent evaluations conducted by agency IGs include an assessment of the effectiveness of the agency's information security policies and practices, as opposed to just an assessment of agency compliance with FISMA requirements and OMB guidelines.[132] The law also required agencies to provide notice to Congress within seven days of a major cybersecurity incident, with OMB defining what constitutes a "major" incident.[133]

A significant change from FISMA 2002 to FISMA 2014 was codification of DHS' responsibilities as they relate to federal cybersecurity. FISMA 2014 authorized DHS to assist OMB in administering agency information security programs through the coordination of government-wide information security efforts, collaboration with NIST, and technical and operational assistance to other federal agencies.[134] Additionally, FISMA 2014 authorized DHS to issue binding operational directives to agencies in order to provide compulsory direction to agencies in the implementation of OMB policies, standards, and guidelines.[135] These directives include instructions for reporting security incidents, details on the type of information to be included in annual reports, and operational standards.[136] However, while FISMA 2014 authorized DHS to provide oversight of cybersecurity operations, it "[does] not authorize the department to take control of networks during emergencies."[137]

---

[131] Caitlin Meade & Susan Cassidy, *FISMA Updated and Modernized*, INSIDE GOV'T CONT. – PROCUREMENT AND POL'Y INSIGHTS (Dec. 19, 2014), http://www.inside governmentcontracts. com/2014/12/fisma-updated-and-modernized (providing a summary of the changes from FISMA 2002 to FISMA 2014).
[132] GAO-15-714, *supra* note 28, at 10-11.
[133] Stacey Banks, *The Federal Information Security Modernization Act of 2014*, TENABLE NETWORK SECURITY (Jan. 16, 2015), https://www.tenable.com/blog/the-federal-information-security-modernization-act-of-2014.
[134] Meade & Cassidy, *supra* note 131.
[135] *Id.*
[136] GAO-15-714, *supra* note 28, at 10.
[137] Aliya Sternstein, *Senators Want Homeland Security to be a Leading Cyberdefense Agency*, NAT'L J. (July 23, 2015), http://www.nationaljournal.com/s/71528/senators-want-homeland-security-be-leading-cyberdefense-agency.

While there has been limited operational time since the enactment of FISMA 2014 to determine the effectiveness of its modernization of FISMA 2002, the changes that Congress made do not address many of the weaknesses of FISMA 2002 (described in depth below). FISMA 2014 still lacked consistent metrics designed to measure the quality and effectiveness of information security programs, as well as an enforcement mechanism or resources to ensure agencies comply with standards and address deficiencies in their cybersecurity programs.

D. Challenges with FISMA

FISMA 2002, and its reformed FISMA 2014 (collectively henceforth, "FISMA"), provided a framework for the implementation of information security controls for federal agencies. However, as a legislative framework, FISMA has ultimately proved to be "too weak to effectively prevent cyber intrusions."[138] Agencies implementing information security programs directed at satisfying the reporting requirements under FISMA will not necessarily see the results in an effective information security program capable of protecting against cyber threats.[139] This is because FISMA establishes a framework to achieve a minimum acceptable level of security, permitting agencies the flexibility to simply satisfy FISMA's reporting requirements without actually implementing a risk management strategy to information security.[140] As a result, in recent years, agencies have experienced a significant increase in the overall number of security incidents, including a more than 1,120

[138] ROLLINS & HENNING, *supra* note 8, at 5.

[139] HOWARD, *supra* note 87, at 27 ("An information security program established and implemented to comply with FISMA can result in an effective program that meets an agency's risk-based needs for security. However, implementing security that aims to satisfy FISMA reporting requirements will not necessarily lead to an effective information security program."). *See also* William Jackson, *Homeland Security Tops FISMA Scorecard. How Do They Do It?*, GCN (June 19, 2014), https://gcn.com/articles/2014/06/19/dhs-oig-fisma-monitoring.aspx ("[C]ompliance does not equal security.").

[140] HOWARD, *supra* note 87, at 27.

percent increase from FY 2006 through FY 2014,[141] demonstrating that federal systems remain at risk and may not actually be more secure under FISMA.

FISMA is a "well-intentioned but fundamentally flawed tool" because it provides a mechanism for information security planning as opposed to serving as an effective method for actually measuring and improving information security.[142] A criticism of FISMA is that agencies and security officials often view the requirements as a "checklist" or "paperwork drill."[143] The assignment of annual letter grades to the 24 major agencies by the House Committee on Government Reform based on the annual FISMA reports has only perpetuated this.[144] Rather than incentivizing agencies to improve information security programs, this report card led agencies to adopt a "check the box" approach to meet FISMA's requirements in order to achieve a passing grade.[145]

Without a strong enforcing mechanism under FISMA, agencies lacked incentives to comply with the statute's requirements, and as such, implementation of cybersecurity programs under FISMA has not consistently occurred across government.[146] "An underlying cause for information security weaknesses . . . is that [agencies] have not yet fully or effectively implemented an agency wide information security program"[147] as required by FISMA. By the start of FY 2006, none of the 24 major agencies had implemented an agency-wide information security program,[148] and by the start of FY

---

[141] GAO-15-714, *supra* note 28, at 11. In FY 2014, the number of information security incidents that federal agencies reported was 67,168, a rise from 41,776 in FY 2010 and 5,503 in FY 2006. *Id.*; GAO-12-137, *supra* note 92, at 4.
[142] William Jackson, *FISMA's Effectiveness Questioned*, GCN (Mar. 18, 2007), https://gcn.com/Articles/2007/ 03/18/FISMAs-effectiveness-questioned.aspx.
[143] *Id.*
[144] *See* William Jackson, *FISMA Grades: What Do They Mean?*, GCN (Apr. 23, 2007), https:// gcn.com/articles/2007/04/23/fisma-grades-what-do-they-mean.aspx.
[145] HOWARD, *supra* note 87, at 30.
[146] *See, e.g.*, Silvers, *supra* note 15, at 1858; William Jackson, *Keith Rhodes: Effective IT Security Starts with Risk Analysis, Former GAO CTO Says*, GCN (June 10, 2009), https:// gcn.com/Articles/2009/06/15/Interview-Keith-Rhodes-IT-security.aspx.
[147] GAO-12-137, *supra* note 91, at 16.
[148] *No Computer System Left Behind: A Review of the 2005 Federal Computer Security Scorecards Before the H. Comm. on Gov't Reform*, 109th Cong. 32 (2006) (statement

2013, still none of the 24 major federal agencies had fully or effectively implemented the entire information security program components required under FISMA.[149] A fully implemented agency-wide information security program would provide the agency with a continuing cycle for assessing risk, developing security policies and procedures, facilitating awareness for information security, and establishing remediation activities to address deficiencies.[150] Failure to implement such a program could lead to inadequate protection of sensitive information.[151] "Until agencies fully resolve identified deficiencies in their agency wide information security programs, the federal government will continue to face significant challenges in protecting its information systems and networks."[152] As further evidence of the slow implementation of FISMA requirements, by the start of FY 2015, over a decade after the enactment of FISMA 2002, only 41 percent of non-Department of Defense agencies had implemented the "Strong Authentication" requirements, which requires agencies to provide employees with enhanced security credentials.[153]

In multiple U.S. Government Accountability Office ("GAO") reports issued since 2008, GAO has identified that, despite agency self-reported progress in implementing FISMA 2002's requirements, "major federal agencies continue to experience significant information security control deficiencies that limit the effectiveness of their efforts to protect the confidentiality, integrity, and availability of their information and information systems."[154]

---

of Gregory C. Wilshusen, GAO Director, Information Security Issues, U.S. Government Accountability Office).

[149] *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-776, FEDERAL INFORMATION SECURITY: MIXED PROGRESS IN IMPLEMENTING PROGRAM COMPONENTS; IMPROVED METRICS NEEDED TO MEASURE EFFECTIVENESS 1, 44-45 (2013) [hereinafter GAO-13-776].

[150] GAO-08-571T, *supra* note 16, at 19.

[151] GAO-12-137, *supra* note 91, at 16.

[152] *Id.*

[153] OMB FY14 FISMA Report, *supra* note 99, at 6-7 (implementation of "Strong Authentication" requires users to log-on to federal networks with unique identification cards).

[154] GAO-08-571T, *supra* note 16, at 3. *See also* GAO-15-714, *supra* note 28, at 11; GAO-12-137, *supra* note 91, at 33.

Additionally, agencies have not adequately overseen the security requirements for information systems operated by federal contractors.[155] By FY 2008, nearly half of agency IGs reported that their agency did not consistently ensure that information systems used by contractors met FISMA requirements, NIST standards, or OMB policies,[156] and by FY 2012, 75 percent of agency IGs identified weaknesses in agency oversight of contractor information systems.[157] GAO concluded that federal systems and information are at an increased risk for unauthorized access to sensitive information, but that agencies could improve their cybersecurity posture by implementing the hundreds of recommendations made by IGs and GAO based on prior evaluations and identified weaknesses.[158]

In many situations, agencies were aware of their cybersecurity issues and information security program weaknesses, but they failed to take sufficient action.[159] For instance, many of the issues with OPM's information security programs were systemic, and OPM's IG had identified them as early as FY 2007.[160] In its FY 2014 annual audit report, the OPM IG summarized its findings based on its evaluation of OPM's information technology security program and practices, identifying material weaknesses related to the information security governance; material weaknesses in the internal control structure of OPM's IT security program; lack of a comprehensive inventory of servers, databases, and network devices; failure to adequately monitor its systems; and failure to adequately test its systems.[161] The IG also identified that, of OPM's 47 major information systems, 38 of these systems had known vulnerabilities

[155] GAO-12-137, *supra* note 91, at 32.
[156] *See* GAO-08-571T, *supra* note 16, at 10.
[157] GAO-12-137, *supra* note 91, at 32.
[158] GAO-08-571T, *supra* note 16, at 3.
[159] *See* GAO-15-714, *supra* note 28, at 11; GAO-12-137, *supra* note 91, at 27-28.
[160] *Is the OPM Data Breach the Tip of the Iceberg?: Hearing Before the Subcomm. on Research & Tech. and Oversight of the Comm. on Sci., Space, and Tech.,* 114th Cong. 3 (2015) (statement of Michael R. Esser, OPM Assistant IG for Audits).
[161] U.S. OFFICE OF PERS. MGMT., OFFICE OF THE INSPECTOR GEN., 4A-CI-00-14-016, FINAL AUDIT REPORT: FEDERAL INFORMATION SECURITY MANAGEMENT ACT AUDIT FY 2014 (2014).

that could potentially lead to data breaches.[162] As the IG stated, "even when [OPM] has known about security vulnerabilities, it has failed to take action."[163] Because of its findings, the IG provided OPM with 29 recommendations to address the information security weaknesses, many of which were recommendations that previous audit reports provided.[164] Ultimately, OPM's IG reported these weaknesses and OPM's failure to manage its information systems and infrastructure culminated in the cyber breaches in June 2015.[165] Even after these attacks, OPM's IG remains concerned that OPM's plans to address the material weaknesses in its information systems will still leave the agency's systems insufficiently protected against future attacks.[166]

Despite the repeated identification of weaknesses, as well as the countless opportunities for improvement, federal agencies are not held accountable for failing to comply with the requirements of FISMA or implementing the recommendations stemming from the annual evaluations of their federal information security programs. A review of OPM's implementation of FISMA demonstrates this lack of accountability associated with an agency's failure to meet FISMA's requirements and provides an example of the consequences that can result. "Too many federal agencies like OPM fail to meet the basic standards of cybersecurity, and no one is being held accountable."[167] The lack of accountability was in part due to the ineffective tools available to OMB to enforce the requirements, but also the decentralized structure for oversight responsibility.[168] Failure to hold

[162] *Is the OPM Data Breach the Tip of the Iceberg?, Hearing Before the Subcomm. on Research & Tech. and Oversight of the Comm. on Sci., Space, and Tech.,* 114th Cong. 7-8 (2015) (statement of Michael R. Esser, OPM Assistant IG for Audits).
[163] *Id.*
[164] *Id.* at 7.
[165] *Id.* at 2.
[166] U.S. OFFICE OF PERS. MGMT., OFFICE OF THE INSPECTOR GEN., 4A-CI-00-15-011, FINAL AUDIT REPORT: FEDERAL INFORMATION SECURITY MANAGEMENT ACT AUDIT FY 2015 (2015).
[167] Zach Noble, *Fixing FISMA, Blaming. . . Someone, and Another Lawsuit*, FCW: THE BUS. OF FED. TECH. (July 9, 2015), https://fcw.com/articles/2015/07/09/opm-breach-hearing.aspx (quoting Rep. Lamar Smith).
[168] *See, e.g.*, Silvers, *supra* note 15, at 1863 ("FISMA vests degrees of responsibility in at least four individuals within each agency: the agency head herself; the agency IG and CIO; and the agency's CIO's specially designated assistant for FISMA. This means that in any given agency at least four senior executives share FISMA oversight

agencies accountable for appropriately managing their information security programs and addressing long-standing cyber issues may lead to a continued increase in cyber attacks on federal systems.

E. Federal Information Security Management Reform Act

In the wake of the OPM cyber incidents, a bi-partisan group of legislators introduced FISMRA 2015, which sought to update FISMA 2014 by providing additional authority to DHS.[169]

> "The attack on OPM has been a painful illustration of just how behind the curve some of our federal agencies have been when it comes to cybersecurity . . . If we want to be better prepared to meet this threat in the future, we have to make sure that [DHS] has the tools it needs to adequately secure our federal civilian networks."[170]

These members of Congress are concerned that, under the current legislation, DHS "does have the 'teeth' to actually enforce security standards or fix vulnerabilities."[171]

The proposed statute would allow DHS to monitor all agency systems using intrusion detection and prevention technology.[172] Under the FISMA 2014 framework, DHS needs permission from an agency in order to investigate or monitor that agency's systems.[173] Under the FISMRA 2015 proposals, DHS would have the authority to monitor agency systems without permission.[174] Using this authority, DHS would be able to conduct risk assessments, as well as

---

responsibility . . . This kind of overlapping and duplicative responsibility breeds the administrative inertia and complacency for which bureaucracies are (in)famous.").

[169] Jason Miller, *Senators Want DHS to Have NSA-Like Defensive Cyber Powers*, FED. NEWS RADIO (July 23, 2015), http://federalnewsradio.com/legislation/2015/07/senators-want-dhs-nsa-like-defensive-cyber-powers.

[170] Sternstein, *supra* note 137 (quoting Sen. Mark Warner) (internal quotation marks omitted).

[171] 161 CONG. REC. S5456 (daily ed. July 22, 2015) (statement of Sen. Warner).

[172] Sternstein, *supra* note 137.

[173] Cory Bennett, *Senators Unveil New Homeland Security Cyber Bill*, THE HILL (July 22, 2015), http://thehill.com/policy/cybersecurity/248775-senators-set-to-unveil-new-dhs-cyber-bill.

[174] *Id.*

scan for and repel attacks, of any network within the dot-gov domain.[175] If DHS detects a threat, they would have the power to direct agencies "to take any lawful action with respect to the operation of the information system at risk."[176]

Under this reform, DHS would have a more significant and military-like role in federal cybersecurity with the authority to intervene and monitor other agencies' information systems and conduct defensive countermeasures to improve cybersecurity.[177] While FISMRA 2015 would take additional steps to protect the federal information infrastructure through increased threat detection and provides a stronger enforcing function via DHS, there are concerns that DHS may not have the capability to satisfy the bill's requirements.[178] Further, the proposed legislation does not address the lack of meaningful metrics designed to measure the effectiveness of information security programs, nor does it provide DHS with sufficient tools to ensure agency compliance with cybersecurity standards.

F. Role of the Executive Branch in Cybersecurity

The Constitution grants the executive and legislative branches authority relating to national security.[179] However, there is some disagreement as to whether the White House has supreme authority and oversight for cybersecurity,[180] or whether this authority is limited to responsibility for cybersecurity emergencies only.[181] Regardless of which branch of government should "own" cybersecurity regulation and enforcement, the executive branch has recently taken more action to address cybersecurity issues because of

---

[175] *See* Miller, *supra* note 169; Sternstein, *supra* note 137 (internal quotation marks omitted).
[176] Sternstein, *supra* note 137.
[177] *See* Miller, *supra* note 169.
[178] *See id.*
[179] ROLLINS & HENNING, *supra* note 8, at 10.
[180] *Id.* at 5 (quoting *Cybersecurity Recommendations for the Next Administration: Hearing Before the Subcomm. on Emerging Threats, Cybersecurity and Sci. and Tech. of the H. Homeland Sec. Comm.*, 110th CONG. 19 (Sept. 16, 2008)).
[181] *See* Fredland, *supra* note 42, at 10.

inaction by Congress and disagreements between these branches and relevant stakeholders about the appropriate action.[182]

In February 2013, President Obama signed Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, in response to repeated cyber attacks of critical infrastructure.[183] This Executive Order had two primary focuses: "cybersecurity information sharing and the development and implementation of risk-based cybersecurity standards for critical infrastructure."[184] It specifically ordered the NIST to lead the development of a cybersecurity framework to reduce cybersecurity risks to critical infrastructure, and it directed the Secretary of Homeland Security to set performance goals within this framework.[185]

The President issued Executive Order 13636 in part due to Congress' inaction and failure to enact cybersecurity legislation.[186] Through this Executive Order, "the White House focused its efforts on critical infrastructure protection, the most controversial part of the comprehensive cybersecurity legislation that failed in the Senate."[187] But critics argued that an Executive Order of this nature was not strong enough to address the issues and only legislation, enacted through the democratic process, would effectively impact the

---

[182] Ferraro, *supra* note 11, at 300 ("The executive branch has taken action to address cybersecurity, recently through an Executive order meant to strengthen public-private cooperation on electronic infrastructure protection, but broader legislation intended to bolster cybersecurity has failed due to disagreements among the U.S. House, Senate, and White House, and privacy advocates, business interests, and security specialists.").

[183] Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013).

[184] Teplinsky, *supra* note 28, at 297.

[185] ERIC A. FISCHER ET AL., CONG. RESEARCH SERV., R42984, THE 2013 CYBERSECURITY EXECUTIVE ORDER: OVERVIEW AND CONSIDERATIONS FOR CONGRESS 8-9 (2014).

[186] *Id.* at 14 ("E.O. 13636 was issued in the wake of the lack of enactment of cybersecurity legislation in the 112th Congress, apparently at least in part as a response to that."). *See also* Ferraro, *supra* note 11, at 300 ("The executive branch has taken action to address cybersecurity, recently through an Executive order meant to strengthen public-private cooperation on electronic infrastructure protection, but broader legislation intended to bolster cybersecurity has failed due to disagreements among the U.S. House, Senate, and White House, and privacy advocates, business interests, and security specialists.").

[187] Teplinsky, *supra* note 28, at 295.

nation's cybersecurity posture.[188] At the very least, this Order was an early step by the executive branch in addressing the nation's cybersecurity challenges.[189]

Nearly two years later, President Obama issued Executive Order 13691, *Promoting Private Cybersecurity Information Sharing*, to encourage private entities to share information related to cybersecurity risks and incidents across the private sector and with the government, with the goal of increasing collaboration to develop mechanisms to improve cybersecurity capabilities and protections.[190] This Executive Order does not impose mandatory requirements on private corporations; rather, it establishes a framework for voluntary information sharing and creates protections from public disclosure to encourage sharing among these entities.[191] As a result, DHS is working to establish best practices for information sharing to aid private corporations in sharing information with each other and the government.[192] But again, this Order is just one step in addressing cybersecurity and, specifically, the sharing of cyber threats, an area where little legislative action has occurred to date.[193]

---

[188] John McCain et al., *No Cybersecurity Executive Order, Please*, WALL ST. J., Sept. 14, 2012, at A13.
[189] *See* J. Nicholas Hoover, *Cybersecurity Executive Order Leaves Tough Work Undone*, INFO. WEEK (Feb. 13, 2013), http://www.darkreading.com/risk-management/cybersecurity-executive-order-leaves-tough-work-undone.
[190] Exec. Order No. 13,691, 80 Fed. Reg. 9,349 (Feb. 13, 2015).
[191] *See* WHITE HOUSE: OFFICE OF THE PRESS SEC'Y, FACT SHEET: EXECUTIVE ORDER PROMOTING PRIVATE SECTOR CYBERSECURITY INFORMATION (Feb. 12, 2015).
[192] *Jeh Johnson on U.S. Cybersecurity Readiness*, COUNCIL ON FOREIGN REL. (Nov. 4, 2015), http://www.cfr.org/homeland-security/jeh-johnson-us-cybersecurity-readiness/p37196 (providing a transcript of a conversation between Jeh Johnson, DHS Secretary, and Andrea Mitchell, Chief Foreign Affairs Correspondent for NBC News, conducted during a Council on Foreign Relations Cybersecurity Symposium).
[193] Ron Gula, *Opinion: Why the "Cyber Bill" Falls Short on Protecting Critical Networks*, THE CHRISTIAN SCI. MONITOR (Oct. 21, 2015), http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/1021/Opinion-Why-the-cyber-bill-falls-short-on-protecting-critical-networks.

IV. RECOMMENDATIONS FOR A FEDERAL CYBERSECURITY LEGISLATIVE FRAMEWORK

This section provides recommendations for modifying the United States federal cybersecurity legislative framework, which includes addressing the challenges identified with current legislation and proposed legislation aimed at regulating federal systems to better guard against cyber threats and improve the protection of the federal information infrastructure. Specifically, this section addresses the need for the legislative framework to be revised to establish meaningful standards for federal information security programs, identification of an enforcement mechanism, as well as the need to ensure federal agencies have the appropriate resources to address cybersecurity weaknesses.

A. Standards: Need for a Clear Framework that Improves Information Systems through Meaningful Metrics and an Accountable Official

Framework legislation for cybersecurity is beneficial in that it provides an overall structure and process within which agencies can operate to address complicated cyber issues.[194] Congress should require definition and enhancement of the standards for agency compliance within the current legislative framework for federal information security to ensure standards are meaningful.[195] "The current metrics do not measure how effectively agencies are performing various activities."[196] As GAO described, agencies must currently test the effectiveness of the security controls of their information systems and include information on the number of systems undergoing these tests in their annual reports, but there is no consistent standard associated with the quality of the tests being conducted across government.[197] Thus, information security metrics associated with FISMA must be modified to be clear and measurable against established performance targets to allow monitoring of progress over time, and they must focus on the quality of agency

[194] *See* Delaney, *supra* note 10, at 267-68.
[195] *See* GAO-12-137, *supra* note 91, at 21.
[196] GAO-08-571T, *supra* note 16, at 27.
[197] *Id.*

performance in implementing security controls and managing risk to their information systems.

However, advances in technology could outpace the government's ability to define and update standards for enforcement. Therefore, OMB and NIST will need to continuously assess and revise these standards against current and emerging cybersecurity risks and threats to ensure they do not become obsolete.[198]

OMB should also clarify how the independent IGs evaluations of agency information security programs are conducted. Currently, there is no common approach or methodology, and thus, IG evaluations vary across agencies.[199] Reporting guidance has been incomplete, and IG responses to the evaluation have been inconsistent as a result.[200] These independent evaluations can serve as an effective method for determining agency compliance with established guidelines and metrics, but consistency in the assessment process and quality control must exist first.

Establishing new standards, or enhancing existing metrics, are not sufficient; these standards must be enforced and agencies must be held accountable for non-compliance. Annual IG evaluations, as well as external organization assessments such as the GAO, have consistently identified weaknesses and provided hundreds of recommendations for improvement,[201] but agencies have been slow to act, in part because of a lack of an enforcement mechanism.

To ensure proper accountability and enforcement across government, cybersecurity legislation should establish a senior accountable official that serves as the individual responsible for ensuring implementation of federal information security requirements. This individual, and supporting resources consisting

---

[198] Gable, *supra* note 30, at 98 ("[I]f better standards and security measures are not continually developed, those working to break security mechanisms will quickly catch up to and surpass those trying to maintain security.").
[199] GAO-08-571T, *supra* note 16, at 28.
[200] *See* GAO-15-714, *supra* note 28, at 52.
[201] *See* GAO-08-571T, *supra* note 16, at 3.

of information security business experts, should reside in OMB to demonstrate the importance of securing and sustaining effective federal systems. When agencies do not comply with established standards or fail to address significant information security program deficiencies, this cyber-accountability official would have the authority to assemble a team of experts from its own office and across government to work directly with the struggling agency to build the necessary framework in an expedient manner. This cyber-accountability official must have the authority to inspect agency information systems and information security programs at any time and without advanced notice. If an agency fails to comply or cooperate, this responsible entity would have the power to enforce sanctions to hold the agency accountable and incentivize action.[202] This provides a "carrot and the stick" approach, with the carrot being assistance to the agency and the stick being sanctions. A cyber-accountability official has the benefit of ensuring uniformity and consistency in the implementation of established standards and allows for identification of lessons learned and the application of best practices across government. At the end of the day, agencies must have the proper incentive to act before another OPM-like incident—or worse—occurs.

B. Resources: Need for Greater Flexibility to Hire Cyber Talent and Consistent Funding for Cybersecurity

But standards, and an individual to enforce these standards, may be insufficient. Federal agencies must have the appropriate resources, both human capital and financial, to develop and sustain effective information security programs to protect the current federal information infrastructure and guard against complex and emerging cyber threats.[203] Without sufficient resources in place to achieve identified targets, information security standards are meaningless.

---

[202] Silvers, *supra* note 15, at 1869 ("Surprise inspections have an established pedigree within the federal administrative state. They have been used successfully in several regulatory contexts as a means of enhancing compliance 'by increasing the likelihood that violations will be detected.'").

[203] *See, e.g.*, Gula, *supra* note 193 ("Success may mean hiring more cybersecurity experts, and/or investing in tools to detect and remediate network vulnerabilities

Government agencies need to be able to recruit and retain a high caliber workforce with the expertise and capabilities necessary to implement and maintain effective information security programs. As the federal government is responsible for protecting its critical information infrastructure and the sensitive information that resides within its networks, it must have the cybersecurity talent in place to accomplish this. However, federal agencies have historically struggled to recruit, hire, retain, and train skilled workers in information technology and cybersecurity fields.[204] "There is a nationwide shortage of highly qualified cybersecurity experts, and the federal government in particular has fallen behind in the race for this talent."[205] This is in part because the federal government lacks a comprehensive or coordinated strategy to recruit and retain a skilled cyber workforce,[206] and many agencies, particularly those with smaller cybersecurity programs, have difficulty recruiting the right talents.[207] The government must establish a comprehensive strategy to address its cybersecurity needs and deficiencies, in alignment with the legislative requirements under FISMA. In turn, reforms to cybersecurity legislation must provide federal agencies with flexibilities to break from the antiquated federal hiring and personnel system through expedited hiring[208] and advanced, market-sensitive compensation to attract and retain the right cyber talent.

Without proper funding, agencies will not be able to support implementation of effective information security programs. Requiring agencies to perform additional work without additional

with fewer personnel. The security industry is experiencing a severe talent drought, so competition for top performers is intense. At the same time, good tools cost money; however the return for the right tool is often worth the initial cost.").

[204] P'SHIP FOR PUB. SERV., CYBER IN-SECURITY II: CLOSING THE FEDERAL TALENT GAP 1 (2015) [hereinafter P'SHIP FOR PUB. SERV., CYBER IN-SECURITY II]; *see also* P'SHIP FOR PUB. SERV., CYBER IN-SECURITY I: STRENGTHENING THE FEDERAL CYBERSECURITY WORKFORCE 1 (2009) [hereinafter P'SHIP FOR PUB. SERV., CYBER IN-SECURITY I].

[205] P'SHIP FOR PUB. SERV., CYBER IN-SECURITY II, *supra* note 204, at 1.

[206] *See id.* at 2.

[207] *See* P'SHIP FOR PUB. SERV., CYBER IN-SECURITY I, *supra* note 204, at 8.

[208] While direct hire authority exists to allow for an expedited hiring process when there is a critical hiring need or severe shortage of qualified candidates, this authority only exists for certain cybersecurity subspecialties and use has been limited. P'SHIP FOR PUB. SERV., CYBER IN-SECURITY II, *supra* note 204, at 14-16.

funds is unlikely to result in compliance with the statute. This was demonstrated after the enactment of FISMA 2002.[209] Specifically, agency heads were required to ensure adequate staffing of trained personnel to support FISMA requirements;[210] however, agencies lacked additional funds for these staffs or other resources to implement FISMA requirements and were expected to improve their cybersecurity posture within the constraints of preexisting budgets.[211]

The amount that agencies spend on information security fluctuates from year to year. From FY 2010 through FY 2014, the 24 major agencies total spending on cybersecurity varied between 10.3 billion dollars (FY 2013) and 14.6 billion dollars (FY 2012),[212] with nearly two-thirds of this dedicated to the Department of Defense.[213] Funding provided to individual agencies for cybersecurity also varies, with factors such as the recent occurrence of a major cyber incident potentially playing a role in that determination. For instance, following the OPM cyber incidents in 2015, OPM received a significant funding increase in FY 2016 compared to FY 2015, which included 21 million dollars (or approximately eight percent of its total budget) devoted to cybersecurity.[214] For comparison, OPM previously spent nearly the lowest amount in federal government on cybersecurity, spending only seven million dollars in FY 2014.[215]

---

[209] Silvers, *supra* note 15, at 1859 ("FISMA does not directly bring new funding to the agencies. So, while agencies must perform more work-often with the assistance of costly private contractors-they must effectively do so within the constraints of their preexisting budgets. For bureaus that already consider themselves strapped for cash, these new tasks may foster reluctance towards implementation, and perhaps even resentment aimed at those ordering the new work to be performed.").

[210] HOWARD, *supra* note 87, at 17.

[211] Silvers, *supra* note 15, at 1859; *see also* HOWARD, *supra* note 87, at 31 ("Agencies were not given additional funding to meet FISMA requirements, but had to reprogram from existing funding to meet the additional information security requirements.").

[212] GAO-15-714, *supra* note 28, at 46.

[213] Gula, *supra* note 193.

[214] Eric Katz, *Winners and Losers in the Omnibus Spending Bill*, GOV'T EXEC. (Dec. 17, 2015), http://www.govexec.com/management/2015/12/winners-and-losers-omnibus-spending-bill/124600.

[215] Mohana Ravindranath, *Before Breach, OPM Requested Millions of Dollars to Upgrade Network Security*, NEXTGOV (June 5, 2015), http://www.nextgov.com/cyber security/2015/06/ breach-opm-requested-32-million-more-cyber/114580.

While the 21 million dollars for cybersecurity at OPM was requested by the agency before the announcement of the recent cyber incidents in June 2015, it is evident that an increase in funding is required for this agency to implement network and information technology infrastructure upgrades and ensure an effective information security program.[216]

"Simply spending more money doesn't automatically make you more secure, but if the U.S. government wants to keep the nation secure and protect America's private data, it must invest more in cybersecurity."[217] Therefore, Congress and OMB should assess the allocation of funds to federal agencies to determine appropriate levels of funding necessary to resolve systemic information security issues and develop information security programs that are capable of responding to complex and emerging cyber threats.

Recognizing that providing agencies with an infinite amount of resources to establish premier information security programs or address long-standing deficiencies in cybersecurity would be impossible, cost-sharing steps should be taken where practicable. Therefore, the use of government-wide activities and common practices should be evaluated to identify areas within the information security realm for cost sharing or use of shared services among federal agencies.

V. CONCLUSION

The United States is unable to adequately protect against the increasingly frequent and sophisticated cyber threats to federal information infrastructures because the nation lacks an effective cybersecurity legislative framework for the regulation of government systems. While FISMA 2002, and its reform in FISMA 2014, provides a framework, it is limited and ineffective at ensuring government agencies adhere to the requirements established by existing statutes. As a result, government entities remain at unnecessary risk and are becoming increasingly susceptible to cyber

[216] *See* U.S. OFFICE OF PERS. MGMT, FY 2016 CONGRESSIONAL BUDGET JUSTIFICATION 2 (2015).
[217] Gula, *supra* note 193.

attack. "It is not a matter of if, but of when government systems will again be hit by a major cyber attack,"[218] and it is critical to our national security that Congress take immediate steps to enact legislation that effectively regulates the cybersecurity of federal systems. Reforms to legislation related to federal cybersecurity must establish a clear, meaningful regulatory framework that includes specific, measurable standards for federal agencies to implement and provides a means for ensuring accountability. Federal agencies must be given appropriate resources—people and dollars—to address systemic cybersecurity weaknesses and develop effective information security programs. Failing to improve the U.S. cybersecurity regulatory framework to ensure adequate protection of federal systems will inevitably result in future cyber attacks of a debilitating nature.

[218] 161 CONG. REC. S5456 (daily ed. July 22, 2015) (statement of Sen. Warner).