



MILITARY LAW REVIEW

ARTICLES

SOLVING THE DILEMMA OF STATE RESPONSE TO CYBERATTACKS: A
JUSTIFICATION FOR THE USE OF ACTIVE DEFENSES AGAINST STATES
WHO NEGLECT THEIR DUTY TO PREVENT

Lieutenant Commander Matthew J. Sklerov

HALLIBURTON HEARS A WHO? POLITICAL QUESTION DOCTRINE
DEVELOPMENTS IN THE GLOBAL WAR ON TERROR AND THEIR IMPACT
ON GOVERNMENT CONTINGENCY CONTRACTING

Major Chad C. Carter

CAPITALIZING "F" IS NOT ENOUGH: THE ARMY SHOULD REVISE ITS
POSTPARTUM LEAVE POLICIES TO BETTER SUPPORT THE ARMY FAMILY

Major Sara M. Root

DON'T ASK, DO TELL: THE IMPLICATIONS OF 2008 CIRCUIT COURT
DECISIONS FOR THE STANDARD OF CONSTITUTIONAL REVIEW APPLICABLE
TO THE MILITARY HOMOSEXUAL CONDUCT POLICY

Major Bailey W. Brown, III

THE SECOND ANNUAL SOLF-WARREN LECTURE IN INTERNATIONAL AND
OPERATIONAL LAW

Professor Ryan Goodman

BOOK REVIEW

MILITARY LAW REVIEW

Volume 201

Fall 2009

CONTENTS

ARTICLES

- Solving the Dilemma of State Response to Cyberattacks: A Justification
for the Use of Active Defenses Against States Who Neglect Their Duty to
Prevent
Lieutenant Commander Matthew J. Sklerov 1
- Halliburton Hears a Who? Political Question Doctrine Developments
in the Global War on Terror and Their Impact on Government
Contingency Contracting
Major Chad C. Carter 86
- Capitalizing “F” Is Not Enough: The Army Should Revise Its Postpartum
Leave Policies to Better Support the Army Family
Major Sara M. Root 132
- Don’t Ask, Do Tell: The Implications of 2008 Circuit Court Decisions for
the Standard of Constitutional Review Applicable to the Military
Homosexual Conduct Policy
Major Bailey W. Brown, III 184
- The Second Annual Solf-Warren Lecture in International and Operational
Law
Professor Ryan Goodman 237

BOOK REVIEW

- Sway: The Irresistible Pull of Irrational Behavior*
Reviewed by *Major Michael D. O’Neil* 262

Headquarters, Department of the Army, Washington, D.C.

Pamphlet No. 27-100-201, Fall 2009

MILITARY LAW REVIEW—VOLUME 201

Since 1958, the *Military Law Review* has been published at The Judge Advocate General's School, U.S. Army, Charlottesville, Virginia. The *Military Law Review* provides a forum for those interested in military law to share the products of their experience and research, and it is designed for use by military attorneys in connection with their official duties. Writings offered for publication should be of direct concern and import to military legal scholarship. Preference will be given to those writings having lasting value as reference material for the military lawyer. The *Military Law Review* encourages frank discussion of relevant legislative, administrative, and judicial developments.

BOARD OF EDITORS

MAJOR ANN B. CHING, *Editor*
MAJOR ALISON M. TULUD, *Assistant Editor*
CPT LAURA A. GRACE, *Assistant Editor*
CPT RONALD T. P. ALCALA, *Assistant Editor*
MR. CHARLES J. STRONG, *Technical Editor*

The *Military Law Review* (ISSN 0026-4040) is published quarterly by The Judge Advocate General's Legal Center and School, 600 Massie Road, Charlottesville, Virginia, 22903-1781, for use by military attorneys in connection with their official duties.

SUBSCRIPTIONS: Interested parties may purchase private subscriptions from the Superintendent of Documents, United States Government Printing Office, Washington, D.C. 20402, at (202) 512-1800. See Individual Paid Subscriptions form and instructions to the *Military Law Review* on pages vi and vii. Annual subscriptions are \$20 each (domestic) and \$28 (foreign) per year. Publication exchange subscriptions are available to law schools and other organizations that publish legal periodicals. Editors or publishers of these periodicals should address inquiries to the Technical Editor of the *Military Law Review*. Address inquiries and address changes concerning subscriptions for Army legal offices, ARNG and USAR JAGC officers, and other federal agencies to the Technical Editor of the *Military Law Review*.

Judge Advocates of other military services should request distribution through their publication channels. This periodical's postage is paid at Charlottesville, Virginia, and additional mailing offices.

POSTMASTER: Send address changes to *Military Law Review*, The Judge Advocate General's Legal Center and School, U.S. Army, 600 Massie Road, ATTN: ALCS-ADA-P, Charlottesville, Virginia, 22903-1781.

CITATION: This issue of the *Military Law Review* may be cited as 201 MIL. L. REV. (page number) (2009). Each issue is a complete, separately-numbered volume.

INDEXING: *Military Law Review* articles are indexed in *A Bibliography of Contents: Political Science and Government; Legal Contents (C.C.L.P.)*; *Index to Legal Periodicals*; *Monthly Catalogue of United States Government Publications*; *Index to United States Government Periodicals*; *Legal Resources Index*; four computerized databases—the JAGCNET, the *Public Affairs Information Service*, *The Social Science Citation Index*, and *LEXIS*—and other indexing services. Issues of the *Military Law Review* are reproduced on microfiche in *Current United States Government Periodicals on Microfiche* by Infodata International Inc., Suite 4602, 175 East Delaware Place, Chicago, Illinois, 60611. The *Military Law Review* is available at <http://www.jagcnet.army.mil/MLR>.

SUBMISSION OF WRITINGS: Anyone may submit for publication consideration, articles, comments, recent development notes, and book reviews in Microsoft Word format to the Senior Editor, *Military Law Review*, at TJAGLCS-MLR-Editor@conus.army.mil. If electronic mail is not available, please forward the submission in duplicate, double-spaced, to the Senior Editor, *Military Law Review*, The Judge Advocate General's Legal Center and School, U.S. Army, Charlottesville, Virginia, 22903-1781. Written submissions must be accompanied by an electronic copy on a 3 1/2 inch computer diskette or CD, preferably in Microsoft Word format.

Footnotes should be typed double-spaced and numbered consecutively from the beginning to the end of the writing, not chapter by chapter. Citations should conform to *The Bluebook, A Uniform System of Citation* (18th ed. 2005), copyrighted by the *Columbia, Harvard, and University of Pennsylvania Law Reviews* and the *Yale Law Journal*, and to the *Military Citation Guide* (TJAGLCS 13th ed. 2008).

Masculine pronouns appearing in the text refer to both genders unless the context indicates another use.

Typescripts should include biographical data concerning the author or authors. This data should consist of branch of service, duty title, present and prior positions or duty assignments, all degrees (with names of granting schools and years received), and previous publications. If submitting a lecture, or a paper prepared in partial fulfillment of degree requirements, the author should include the date and place of delivery of the lecture or the date and source of the degree.

EDITORIAL REVIEW: The *Military Law Review* does not purport to promulgate Department of the Army policy. The opinions and conclusions reflected in each writing are those of the author and do not necessarily reflect the views of the Department of Defense, The Judge Advocate General, the Judge Advocate General's Corps, or any other governmental or non-governmental agency.

The Editorial Board of the *Military Law Review* includes the Chair, Administrative and Civil Law Department, Lieutenant Colonel Craig E. Merutka; and the Director, Professional Writing Program, Lieutenant Colonel Jonathan Howard. The Editorial Board evaluates all material submitted for publication, the decisions of which are subject to final approval by the Dean, The Judge Advocate General's School, U.S. Army. We accept submissions from military and civilian authors, irrespective of bar passage or law school completion. In determining whether to publish an article, note, or book review, the Editorial Board considers the item's substantive accuracy, comprehensiveness, organization, clarity, timeliness, originality, and value to the military legal community. No minimum or maximum length requirement exists.

When the Editorial Board accepts an author's writing for publication, the Editor of the *Military Law Review* will provide a copy of the edited text to the author for prepublication approval. Minor alterations may be made in subsequent stages of the publication process without the approval of the author.

Reprints of published writings are not available. Authors receive complimentary copies of the issues in which their writings appear. Additional copies usually are available in limited quantities. Authors may request additional copies from the Technical Editor of the *Military Law Review*.

BACK ISSUES: Copies of recent back issues are available to Army legal offices in limited quantities from the Technical Editor of the *Military Law Review* at TJAGLCS-Tech-Editor@conus.army.mil. Bound copies are not available and subscribers should make their own arrangements for binding, if desired.

REPRINT PERMISSION: Contact the Technical Editor, *Military Law Review*, The Judge Advocate General's Legal Center and School, U.S. Army, ATTN: ALCS-ADA-P, Charlottesville, Virginia, 22903-1781.

INDIVIDUAL PAID SUBSCRIPTIONS TO THE *MILITARY LAW REVIEW*

The Government Printing Office offers a paid subscription service to the *Military Law Review*. To receive an annual individual paid subscription (4 issues), complete and return the order form on the next page.

RENEWALS OF PAID SUBSCRIPTIONS: You can determine when your subscription will expire by looking at your mailing label. Check the number that follows "ISSDUE" on the top line of the mailing label as shown in this example:

When this digit is 7, you will be sent a renewal notice.



The numbers following ISSDUE indicate how many issues remain in the subscription. For example, ISSDUE001 indicates a subscriber will receive one more issue. When the number reads ISSDUE000, you have received your last issue and you must renew.

To avoid a lapse in your subscription, promptly return the renewal notice with payment to the Superintendent of Documents. If your subscription service is discontinued, simply send your mailing label from any issue to the Superintendent of Documents with the proper remittance and your subscription will be reinstated.

INQUIRIES AND CHANGE OF ADDRESS INFORMATION: The Superintendent of Documents is solely responsible for the individual paid subscription service, not the Editors of the *Military Law Review* in Charlottesville, Virginia.

For inquires and change of address for individual paid subscriptions, fax your mailing label and new address to (202) 512-2250, or send your mailing label and new address to the following address:

United States Government Printing Office
Superintendent of Documents
ATTN: Chief, Mail List Branch
Mail Stop: SSOM
Washington, DC 20402



Order Processing
 Code: 5937

Army Lawyer and Military Review SUBSCRIPTION ORDER FORM

Easy Secure Internet: **bookstore.gpo.gov** Toll Free: 855 612-1800 Mail: Superintendent of Documents
 Phone: 202 512-1800 PO Box 371924
 Fax: 202 512-2104 Pittsburgh, PA 15250-7954

YES, enter my subscription(s) as follows:

_____ subscription(s) of the *Army Lawyer* (ARLAW) for \$50 each (\$70 foreign) per year.

_____ subscription(s) of the *Military Law Review* (MILR) for \$20 each (\$28 foreign) per year. The total cost of my order is \$_____.

Prices include first class shipping and handling and is subject to change.

Personal name _____ (Please type or print)

Company name _____

Street address _____
 City, State, Zip code _____

Daytime phone including area code _____

Purchase Order Number _____



Check method of payment:

- Check payable to Superintendent of Documents
- SOD Deposit Account

--	--	--	--	--	--	--	--	--	--
- VISA MasterCard Discover/NOVUS American Express

--	--	--	--	--	--	--	--	--	--	--	--

(expiration date)

Thank you for your order!

 Authorizing signature

MILITARY LAW REVIEW

Volume 201

Fall 2009

SOLVING THE DILEMMA OF STATE RESPONSES TO CYBERATTACKS: A JUSTIFICATION FOR THE USE OF ACTIVE DEFENSES AGAINST STATES WHO NEGLECT THEIR DUTY TO PREVENT

LIEUTENANT COMMANDER MATTHEW J. SKLEROV*

*How do you account for your discoveries? Through
intuition or inspiration?¹*

*Both. . . I'm enough of an artist to draw freely on my
imagination, which I think is more important than
knowledge. Knowledge is limited, imagination encircles
the world.²*

I. Introduction

The greatest advances in law, like those in science, come through imagination. When scientific knowledge fails to explain new discoveries

* Judge Advocate, U.S. Navy. Presently assigned as Staff Judge Advocate, Submarine Group NINE. LL.M., 2009, The Judge Advocate Gen.'s Legal Ctr. & Sch., U.S. Army, Charlottesville, Va.; J.D., 2002, Univ. of Tex. Sch. of Law; B.A., 1997, State Univ. of N.Y. at Binghamton (*cum laude*); A.A., 1995, State Univ. of N.Y. at Rockland. Previous assignments include Deputy Command Judge Advocate, U.S.S. *Nimitz* (CVN 68), 2006–2008; Command Judge Advocate, Naval Air Station, Kingsville, Tex., 2004–2006; Trial Counsel, Trial Service Office West, Detachment Bremerton, Wash., 2003–2004. Member of the bars of Texas, the U.S. District Court for the Southern District of Texas, the U.S. Court of Appeals for the Armed Forces, and the U.S. Supreme Court. This article was submitted in partial completion of the Master of Laws requirements of the 57th Judge Advocate Officer Graduate Course. The author would like to thank Major J. Jeremy Marsh, U.S. Air Force, for his invaluable assistance with this article.

¹ George Sylvester Viereck, *What Life Means to Einstein: An Interview by George Sylvester Viereck*, PHILA. SATURDAY EVENING POST, Oct. 29, 1929, at 113 (questioning Albert Einstein about his discoveries).

² *Id.* at 117 (quoting Albert Einstein's response to his questions).

about the universe, scientists advance new theories to account for their discoveries—so too with the law. Revolutions in technology, like the Internet, challenge the framework that regulates international armed conflict. Legal scholars must use imagination to find ways to tackle this problem. If not, the law will become obsolete and meaningless to the states that need its guidance.

Man has long sought to regulate warfare. From the Chivalric Code to the Charter of the United Nations (U.N. Charter), man has placed restraints on the times one can resort to war and the methods with which it is conducted. To generalize, regulations are the response to perceived problems with the state of war at a given time. Sometimes these perceptions are the result of shifts in the social conscience. At other times, values have not changed, but problems arise due to radical changes in the way war is waged.

As warfare changes, so must the law, and warfare is changing fast. Traditionally, the instruments of war were controlled only by states. However, in today's world of globally interconnected computer systems, non-state actors with a laptop computer and an Internet connection can attack the critical infrastructure³ of another state from across the world. This is a major paradigm shift, which the law of war today fails to adequately address.

This article will explore the unique challenges that cyberattacks⁴ pose to the law of war and provide an analytical framework for dealing with them. Once the current state of the law of war is fully explored, this article will conclude that states have a right under international law to (1) view and respond to cyberattacks as acts of war and not solely as criminal matters, and (2) use active, not just passive, defenses⁵ against

³ Critical infrastructure are those “systems and assets, whether physical or virtual, 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, [and] national public health or safety.” Critical Infrastructure Protection Act of 2001, 42 U.S.C.S. § 5195c(e) (LexisNexis 2009).

⁴ This article uses derivatives of the root word “cyber,” such as cyberattack, cyberthreat and cyberwarfare. “Cyber” may be used as an adjective that means relating to computers or computer networks. So, a cyberattack would be an attack carried out against a computer or computer network; a cyberthreat would be a threat to a computer or computer network. Merriam-Webster Online Dictionary, <http://www.merriam-webster.com/dictionary/cyber> (last visited Mar. 22, 2009).

⁵ Active defenses are electronic countermeasures designed to strike attacking computer systems, shut them down, and stop a cyberattack midstream. Eric Jensen, *Computer*

the computer networks in other states, that may or may not have initiated an attack, but have neglected their duty to prevent cyberattacks from within their borders.

These conclusions are demonstrated over the next seven parts of this article. Part II provides background on the threat that international cyberattacks pose to states, the legal problems that states encounter when dealing with them, and why current interpretations of the law of war actually endanger states. Part III describes cyberattack methods, destructive capabilities, and defenses. Part IV lays out the basic framework for analyzing armed attacks. Part V explores the challenges that non-state actors present to the basic framework of the law of war. Part VI analyzes cyberattacks under the law of war. It demonstrates that cyberattacks can qualify as acts of war, that states have a duty to prevent cyberattacks, and that victim-states have a right to use active defenses against host-states that neglect their duty to prevent cyberattacks. Part VII examines the choice to use active defenses. It explains why states should use active defenses against cyberattacks, describes the technological limits to detecting, classifying and tracing cyberattacks, and explores the impact these technological limitations will have on state decision making. Finally, Part VIII urges states to start using active defenses to protect themselves from cyberattacks originating from states that neglect their duty to prevent them.

II. Cyberattacks, a Growing International Threat

The Internet is essential to every modern country in the world. It is a cornerstone of commerce.⁶ Strategic government activities are directed through it.⁷ Energy production and distribution, water treatment facilities, mass transit, and emergency services are controlled through it.⁸ The more developed a country is, the more it depends on it.⁹ Indeed,

Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense, 38 STAN. J. INT'L L. 207, 230 (2002). Passive defenses are the traditional forms of computer security used to defend computer networks, such as system access controls, data access controls, security administration, and secure system design. *Id.*

⁶ See ANDREW COLARIK, CYBER TERRORISM: POLITICAL AND ECONOMIC IMPLICATIONS viii–xi (2006) (noting that trillions of dollars of electronic banking and global stock trading are conducted over the Internet each year).

⁷ *Id.*

⁸ *Id.*

⁹ *Id.* at xii.

networked computers have become the nervous system of modern society.¹⁰

Global connectivity, however, is a double-edged sword. While it provides tremendous benefits to states, it also opens the door to state and non-state actors who wish to attack and disrupt a state's critical information systems.¹¹ Furthermore, these attacks can have catastrophic consequences, such as bringing a state's economy to its knees, weakening its national defense posture, or causing the loss of life.¹² While these doomsday scenarios may seem farfetched, the reality is that catastrophic cyberattacks are more likely to occur as states grow more reliant on the Internet,¹³ as terrorists increasingly look to use cyberattacks against states,¹⁴ and as cyberattacks become more frequent and potent.¹⁵

No state is safe from cyberattacks. Recent high-profile cyberattacks highlight such vulnerability. In July 2008, shortly before armed conflict broke out between Russia and Georgia, hackers barraged Georgia's

¹⁰ THE WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE vii (2003) [hereinafter CYBERSPACE NAT'L STRATEGY].

¹¹ COLARIK, *supra* note 6, at xii.

¹² CYBERSPACE NATIONAL STRATEGY, *supra* note 10, at 6–7 (2003); *see also infra* Part III.B.

¹³ *See* Richard Garnett & Paul Clarke, *Cyberterrorism: A New Challenge for International Law*, in ENFORCING INTERNATIONAL LAW NORMS AGAINST TERRORISM 465, 487 (Andrea Bianchi ed., 2004); DANA SHEA, CONG. RESEARCH SERV. REPORT, CRITICAL INFRASTRUCTURE: CONTROL SYSTEMS AND THE TERRORIST THREAT, RL 31534, at CRS-1 to CRS-3 (2003).

¹⁴ *See* SHEA, *supra* note 13, at CRS-6 to CRS-7; *see also* L. Gordon Crovitz, *Internet Attacks are a Real and Growing Problem*, WALL STREET J., Dec. 15, 2008, at 17 (describing terrorist attempts to trick military computers into mistaking the identities of friendly and unfriendly forces in Afghanistan and Iraq).

¹⁵ *See* CLAY WILSON, CONG. RESEARCH SERV. REPORT, BOTNETS, CYBERCRIME, AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS, RL 32114, at CRS-7 to CRS-8 (2007) (noting cyberattacks are growing more frequent due to the use of automated attack programs; cyberattacks now happen so often the Computer Emergency Response Team Coordination Center gave up tracking them, after tracking several hundred thousand successful attacks a year for several years); JOHN ROLLINS & CLAY WILSON, CONG. RESEARCH SERV. REPORT, TERRORIST CAPABILITIES FOR CYBERATTACK: OVERVIEW AND POLICY ISSUES, RL 33123, at CRS-17 (2007) (reporting that the Department of Defense experiences more than three million scans of its computer systems each day by potential attackers, and that according to a study by IBM in 2005, roughly 237 million cyberattacks were conducted globally in the first half of the year); John Markoff, *Internet Attacks Grow More Potent*, N.Y. TIMES, Nov. 10, 2008, at B8 (describing the increasing capabilities of distributed-denial-of-service attacks to shut down computer systems and overcome computer defenses).

Internet infrastructure with coordinated cyberattacks.¹⁶ The attacks overloaded and shut down many of Georgia's computer servers, and impaired Georgia's ability to disseminate information to its citizens during its armed conflict with Russia.¹⁷ In June 2007, Chinese hackers disabled 1500 Pentagon computers, including those of the Secretary of Defense.¹⁸ In April 2007, cyberattacks from Russia crippled the Estonian government and commercial computer networks.¹⁹ These attacks lasted approximately three weeks, disrupted Estonia's ability to govern, harmed Estonia's economy, and damaged their networks so badly that Estonia had to reach out to its NATO allies for help recovering.²⁰ These are some of the more egregious international cyberattacks; however, there have been numerous others, often with severe consequences to the victim-states.²¹ Given the potentially

¹⁶ John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES, Aug. 13, 2008, at A1.

¹⁷ *Id.*

¹⁸ Mark Hosenball, *Whacking Hackers*, NEWSWEEK, Oct. 15, 2007, at 10.

¹⁹ Mark Landler & John Markoff, *After Computer Siege on Estonia, War Fears Turn to Cyberspace*, N.Y. TIMES, May 29, 2007, at A1; James Sterngold, *U.S. on Guard Against Computer Attacks; Estonia's Disruption Shows Need to Fortify Internet's Defenses*, S.F. CHRON., June 24, 2007, at A4.

²⁰ Landler & Markoff, *supra* note 19, at A1; WILSON, *supra* note 15, at CRS-7 to CRS-8.

²¹ See, e.g., Siobhan Gorman et al., *Computer Spies Breach Fighter Jet Projects*, WALL STREET J., Apr. 21, 2009, at A1 (describing Chinese cyberattacks against the U.S. Joint Strike Fighter project); Siobhan Gorman, *Electric Grid in U.S. Penetrated by Spies*, WALL STREET J., Apr. 8, 2009, at A1 (describing Chinese cyberattacks against U.S. electric grids); Christopher Rhoads, *Kyrgyzstan Knocked Offline*, WALL STREET J., Jan. 28, 2009, at 10 (discussing the January 2009 denial-of-service attacks from Russia which effectively knocked Kyrgyzstan offline); Julian Barnes, *Cyber Attack Has Pentagon Worried: Russia Eyed in Hit on Defense Networks*, CHI. TRIB., Nov. 30, 2008, at C16 (discussing the November 2008 cyberattacks from Russia which disrupted U.S. Central Command's classified computer networks); Demetri Sevastopulo, *Chinese Hackers Penetrate White House Network*, FIN. TIMES ONLINE, Nov. 7, 2008, http://www.ft.com/cms/s/0/f16027f0-ac6e-11dd-bf71-000077b07658.html?nclick_check=1 (discussing the cyberattacks from China that penetrated the White House's computer network in autumn 2008, and the Obama and McCain presidential campaign networks in summer 2008); Rhys Blakely et al., *M15 Alert on China's Cyberspace Spy Threat*, TIMES ONLINE, Dec. 1, 2007, http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article2980250.ece (discussing the November 2007 cyberattacks from China against vital British commercial, governmental, and military systems); Liam Tung, *China Accused of Cyberattacks on New Zealand*, CNET NEWS.COM, Sept. 13, 2007, http://news.cnet.com/China-accused-of-cyberattacks-on-New-Zealand/2100-7348_3-6207678.html (discussing the September 2007 cyberattacks from China against New Zealand's government networks); *Merkel's China Visit Marred by Hacking Allegations*, DER SPIEGEL ONLINE, Aug. 27, 2007, <http://www.spiegel.de.international/world/0,1518,502169,00.html> (discussing the August 2007 cyberattacks from China against Germany's government); Roger Boyes, *China Accused of Hacking into Heart of Merkel Administration*, TIMES ONLINE, Aug. 27, 2007,

catastrophic consequences of cyberattacks, it is imperative for states to be able to effectively defend themselves.

A. The Legal Dilemma of State Responses to Cyberattacks

Unfortunately, state responses to cyberattacks are governed by an anachronistic legal regime that impairs a state's ability to defend itself. No comprehensive treaty exists to regulate international cyberattacks.²² Consequently, states must practice law by analogy: either equating cyberattacks to traditional armed attacks and responding to them under the law of war or equating them to criminal activity and dealing with them as a criminal matter.²³ The prevailing view of states and legal scholars is that states must treat international cyberattacks as a criminal matter because the law of war forbids states from responding with force unless an attack can be attributed to a foreign state or its agents.²⁴ This limited view of the law of war is problematic for two reasons. First, it confines state computer defenses to passive defenses, which reduce a

<http://www.timesonline.co.uk/tol/news/world/europe/article2332130.ece> (discussing the August 2007 Chinese cyberattacks against Germany's government); *see also* Richard Behar, *World Bank Under Cyber Siege in "Unprecedented Crisis,"* FOX NEWS.COM, Oct. 10, 2008, <http://www.foxnews.com/story/0%2C2933%2C435681%2C00.html> (showing the vulnerability of intergovernmental organizations to cyberattacks by discussing Chinese cyberattacks against the World Bank).

²² *See* AHMAD KAMAL, *THE LAW OF CYBER-SPACE: AN INVITATION TO THE TABLE OF NEGOTIATIONS* 170–89 (2005); Duncan Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1024–38 (2007); Jon Jurich, *Cyberwar and Customary International Law: The Potential of a "Bottom-up" Approach to an International Law of Information Operations*, 9 CHI. J. INT'L L. 275, 283 (2008). A Convention on Cybercrime was adopted by the Council of Europe, which went into effect in 2004; however, it does not provide a comprehensive structure for dealing with cyberattacks. The United States is the only non-European nation that is a party to the convention. Notably, despite being part of the Council of Europe, Russia never entered the treaty; neither has China. *See* Council of Europe, *Convention on Cybercrime, opened for signature* Nov. 23, 2001, 41 I.L.M. 282 [hereinafter *Convention on Cybercrime*].

²³ *See* Hollis, *supra* note 22, at 1024–38.

²⁴ *See* LAWRENCE GREENBERG ET AL., *INFORMATION WARFARE AND INTERNATIONAL LAW* 83–84 (1997); WALTER GARY SHARP SR., *CYBERSPACE AND THE USE OF FORCE* 8 n.14 (1999); Sean Condon, *Getting it Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J.L. & TECH. 404, 414–15 (2007); Daniel Creekman, *A Helpless America? An Examination of the Legal Options Available to the United States in Responding to Varying Types of Cyber-Attacks from China*, 17 AM. U. INT'L L. REV. 641, 653–54 (2002); Yoram Dinstein, *Computer Network Attacks and Self-Defense*, in *COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW* 99, 111 (Michael N. Schmitt & Brian T. O'Donnell eds., Naval War College 2002).

state's ability to stop cyberattacks.²⁵ Second, it forces states to rely on criminal laws to deter cyberattacks, which are ineffective because several major states are unwilling to extradite or prosecute their attackers.²⁶ Given these problems with the prevailing view, states will undoubtedly find themselves in a "response crisis"²⁷ during a cyberattack, forced to decide between effective, but arguably illegal, active defenses, and the less effective, but legal, path of passive defenses and criminal laws.²⁸

The current legal paradigm, which requires attribution to a state or its agents, perpetuates the response crisis because it is virtually impossible to attribute a cyberattack during an attack. Although states can trace the cyberattack back to a computer server in another state, conclusively ascertaining the identity of the attacker requires an intensive, time-consuming investigation with assistance from the state of origin.²⁹ Given the prohibition on responding with force until an attack has been attributed to a state or its agents, coupled with the fact that the vast majority of cyberattacks are conducted by non-state actors,³⁰ it should come as no surprise that states treat cyberattacks as a criminal matter.³¹ This "attribution problem"³² locks states into the response crisis.

²⁵ Active defenses are one of the most effective defenses to cyberattacks, and can stop them in situations where passive defenses cannot. See Noah Shachtman, *Air Force Aims to "Re-Write Laws of Cyberspace,"* WIRED NEWS, Nov. 3, 2008, <http://blog.wired.com/defense/2008/11/air-force-aims.html>; Crovitz, *supra* note 14, at 17. Ideally, states would defend themselves with a layered defense of active and passive defenses. However, states currently confine their defenses to passive defenses because active defenses cannot be legally used unless force is authorized under the law of war. See Jensen, *supra* note 5, at 231.

²⁶ See *infra* notes 41–46 and accompanying text.

²⁷ "Response crisis" refers to the dilemma that states face in choosing an appropriate response to a cyberattack.

²⁸ Adding pressure to the response crisis is that delaying the use of active defenses will increase the overall risk to a state. See Lord: *Attack Attribution, Intent are Badly Needed Cyberwar Capabilities*, 29 INSIDE A.F., No. 26, June 27, 2008 (quoting Major General William Lord, Commander (Prospective), Air Force Cyber Command); see also Condon, *supra* note 24, at 407–08 (noting that delaying the use of active defenses, so that attacks can be attributed, can result in lost lives and massive damage).

²⁹ See Jensen, *supra* note 5, at 232–35 (discussing the difficulty of attributing cyberattacks across international borders); Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. INT'L L. & POL. 57, 97–99 (2001) (noting that attributing cyberattacks cannot be done without extensive investigation, in which access to the originating servers is granted by the host-state's government).

³⁰ Jensen, *supra* note 5, at 232.

³¹ See Condon, *supra* note 24, at 407 (noting the United States treats international cyberattacks as a criminal matter); Hollis, *supra* note 22, at 1050 (noting that Estonia responded to the 2007 cyberattacks from Russia through diplomatic channels, despite

The high-profile cyberattacks discussed earlier highlight the link between the attribution problem and response crisis. In 2008, Georgia traced the cyberattacks against it back to Russia, but could not pin them on its government.³³ Similarly, U.S. officials believed that China sponsored the 2007 cyberattacks against the Pentagon, but could not prove the link.³⁴ Following a familiar pattern, Estonia traced the 2007 attacks back to Russia, but could not tie them to the Russian government.³⁵ Ultimately, in each of these cases, states were unable to solve the attribution problem, which legally limited them from using active defenses and forced them to rely on passive defenses and criminal laws.

Treating cyberattacks as a criminal matter would not be problematic if passive defenses and criminal laws provided sufficient protection from cyberattacks. Unfortunately, neither is adequate. While passive defenses are always the first line of defense and reduce the chances of a successful cyberattack,³⁶ states cannot rely on them to completely secure their critical information systems.³⁷ Furthermore, passive defenses do little to dissuade attackers³⁸ from attempting their attacks in the first place.³⁹

their belief that Russia sponsored the attacks, because of the legal requirement to attribute cyberattacks before treating them as violations of the law of war).

³² “Attribution problem” refers to the difficulty of ascertaining the identity of cyberattackers.

³³ Markoff, *supra* note 16, at A1. Evidence obtained much later suggests that a criminal gang, known as the Russian Business Network, was behind the cyberattacks with the support of the Russian government. *Id.* See generally Eneken Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, NATO COOPERATIVE CYBER DEFENSE CENTER OF EXCELLENCE (2008) (providing more detailed information on the cyberattacks).

³⁴ Demetri Sevastopulo, *Chinese Hacked into Pentagon*, FIN. TIMES ONLINE, Sept. 3, 2007, <http://www.ft.com/cms/s/0/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac.html>; Demetri Sevastopulo, *Beware: Enemy Attacks in Cyberspace*, FIN. TIMES ONLINE, Sept. 3, 2007, <http://www.ft.com/cms/s/0/a89c1c88-5a38-11dc-9bcd-0000779fd2ac.html>.

³⁵ Landler & Markoff, *supra* note 19, at A1.

³⁶ See LEHTINEN ET AL., *COMPUTER SECURITY BASICS* 3–21 (2d ed. 2006); COLARIK, *supra* note 6, at 10.

³⁷ See COLARIK, *supra* note 6, at 163.

³⁸ Up to this point, the term “hacker” has been used to generically refer to anyone conducting a cyberattack. However, from this point this article will either use the more appropriate term “attacker” to generally refer to individuals who conduct cyberattacks, or one of the more specific terms: “hacker,” “cracker,” “cybercriminal,” and “cyberterrorist.” Hackers are anyone with an eagerness to experiment with computers and test their limits. Crackers are hackers who unlawfully break into systems, usually for the thrill of it, but also to peek at interesting data contained in the systems targeted. Cybercriminals are crackers who go one step further and use their cyberattacks to steal

Deterrence comes from criminal laws and the penalties associated with them.⁴⁰ However, when states fail to pass stringent criminal laws or look the other way when attackers strike rival states, criminal laws are rendered impotent.⁴¹

Unfortunately, several major states refuse to take part in international efforts to eliminate cyberattacks and seem unlikely to start doing so in the near future.⁴² For instance, despite Chinese and Russian pledges to crackdown on their attackers,⁴³ no one has been brought to justice for any of the attacks discussed. China, in fact, conducts training for its hackers

and sell data, embezzle money, or engage in extortion. Cyberterrorists employ cyberattacks to create fear or violence through the destruction or disruption of computer systems, as a means of influencing a government or population to conform to a particular political or ideological agenda. See LEHTINEN ET AL., *supra* note 36, at 16–17; COLARIK, *supra* note 6, at 37–48.

³⁹ In the case of hackers and crackers, beating security measures is often seen as a fun challenge. See LEHTINEN ET AL., *supra* note 36, at 16–17; Frontline: Hacker Interviews, <http://www.pbs.org/wgbh/pages/frontline/shows/hackers/interviews/> (last visited Mar. 22, 2009). Furthermore, the more secure a system is, the more difficult it is for an attacker to penetrate the system's defenses; however, defensive measures alone pose little risk to the attacker. While defensive measures can trace attacks back to their source, absent stringent criminal laws and vigorous law enforcement defensive measures cannot harm an attacker. See COLARIK, *supra* note 6, at 40–45.

⁴⁰ See COLARIK, *supra* note 6, at 39.

⁴¹ CYBERSPACE NAT'L STRATEGY, *supra* note 10, at 8 (2003). State cooperation is essential to the criminal prosecution of international attackers. *Id.* However, state cooperation relies on the goodwill of nations. For instance, even when an attacker has been identified, the host-state may refuse to prosecute or extradite them back to the victim-state. Such obligations only arise from international treaties that set forth state responsibilities. See *Factor v. Laubenheimer*, 290 U.S. 276, 287 (1933); GREENBERG ET AL., *supra* note 24, at 69–72; KAMAL, *supra* note 22, at 215–22. Obtaining state cooperation often requires intense diplomatic activity, which presents its own challenges to relying on host-state criminal laws. For instance, diplomatic activity is usually required to get a host-state to prosecute an attacker under their criminal laws, or to get a host-state to turn over an attacker so that he can be prosecuted under victim-state's criminal laws; neither of which can be required absent a treaty requiring such action. It is worth noting that the United States does not have extradition treaties with China or Russia, and thus no legal right exists to demand the extradition from those states. See Creekman, *supra* note 24, at 658.

⁴² See Condron, *supra* note 24, at 414.

⁴³ See Richard McGregor & Hugh Williamson, *Beijing Pledges Crackdown on International Hackers*, FIN. TIMES ONLINE, Aug. 28, 2007, <http://www.ft.com/cms/s/0/9b4cfc4e-54fe-11dc-890c-0000779fd2ac.html>; Iain Thomson, *Russia Promises Piracy Crackdown*, VNUNET.COM, Mar. 19, 2007, <http://www.vnunet.com/vnunet/news/2185839/russia-promises-piracy> (reporting Russia's pledge to crackdown on online criminal activity).

at its military academies.⁴⁴ Furthermore, security experts believe that China intentionally ignores the criminal acts of its hackers, buys stolen information from them, and uses them to spy on other states.⁴⁵ Meanwhile, Russia has rejected numerous Estonian requests to help track down the attackers responsible for the 2007 cyberattacks.⁴⁶ As may be expected, China and Russia reject these accusations.⁴⁷ Still, all of this suggests that state cooperation is offered in name only, that these states are sponsoring cyberattacks, and that states cannot rely on criminal laws to eliminate the growing cyberthreat. The foregoing discussion illustrates the need to ascertain what states may legally do to defend themselves.

B. The Importance of Using Active Defenses

To escape this dilemma, states must use active defenses. Not only will active defenses greatly decrease the chance of a successful cyberattack, but it also logically follows that attackers will hesitate to attack a state when they know their attacks will be met with a forceful response. After all, “[m]aintaining a credible ability to use force, in cyberspace and elsewhere, is . . . a fundamentally important aspect of deterrence.”⁴⁸ But can states legally act in this manner? Even if so, is this the best way to address the cyberthreat?

⁴⁴ See generally U.S.-CHINA ECON. & SEC. REVIEW COMM’N, 2008 REPORT TO CONGRESS (2008), available at <http://www.uscc.gov> (describing China’s initiatives to augment its cyberwarfare capabilities to gain an advantage over the United States in any future conflict, amid other economic and security concerns).

⁴⁵ See Schneier on Security, http://www.schneier.com/blog/archives/2008/07/chinese_cyber_a.html (July 14, 2008, 07:08 EST) (speculating that China knows its leading hackers, intentionally ignores their international crimes, and even buy stolen intelligence from them).

⁴⁶ See Hollis, *supra* note 22, at 1026. Lending credence to Estonian assertions that Russia is intentionally obstructing the criminal investigation is the fact that the Russian public has hailed the hackers responsible for the cyberattacks against Estonia as national heroes. See Clifford Levy, *What’s Russian for “Hacker”?*, N.Y. TIMES (Week in Review), Oct. 21, 2007, at p. 1.

⁴⁷ Assoc. Press, *China Dismisses U.S. Espionage Report as Misleading*, Nov. 22, 2008, available at <http://abcnews.go.com/International/wireStory?id=6312145>; Richard McGregor & Demetri Sevastopulo, *China Denies Hacking into Pentagon*, FIN. TIMES ONLINE, Sept. 4, 2007, <http://www.ft.com/cms/s/0/a625db16-54c4-11dc-890c-0000779fd2ac.html>; Hollis, *supra* note 22, at 1026.

⁴⁸ SHARP, *supra* note 24, at 135; see THOMAS WINGFIELD, THE LAW OF INFORMATION CONFLICT, NATIONAL SECURITY LAW IN CYBERSPACE 361 (2000).

History shows that states will take matters into their own hands when legal means seem inadequate to protect themselves and their citizens.⁴⁹ One can imagine a scenario where a state was subject to a cyberattack so severe that it felt an armed response was required. Given the ease with which a non-state actor could trigger such a scenario, international law must provide states acceptable legal means to defend themselves. When states have legal means to resolve their disputes, they are more likely to behave in predictable ways that are accepted by the international community.⁵⁰ Thus, unless the international community wants to risk unpredictable and potentially unacceptable responses to cyberattacks, international law must adapt to provide states with legal means to effectively defend themselves.

This is not a new thought. Legal scholars are increasingly recognizing that the current legal regime leaves states vulnerable to cyberattacks and needs to change.⁵¹ However, despite their recognition of the problem, no consensus has emerged on the best way to solve it. Some scholars advocate new treaties to get past this legal shortcoming. For example, one proposal calls for a treaty requiring states to rebuild the Internet's architecture in a more secure manner, so that law enforcement

⁴⁹ This happened in 2008, when the United States authorized its military to carry out air and ground assaults against al Qaeda inside other states without the approval of their governments. Since then, the United States has conducted raids inside Pakistan and Syria against their wishes. The United States justified its actions as self-defense due to those states' inability or unwillingness to handle the terrorists, despite evidence that Pakistan and Syria were cooperating and having some success with their counter-terrorism efforts. See Eric Schmitt & Mark Mazzetti, *Bush Said to Give Orders Allowing Raids in Pakistan*, N.Y. TIMES, Sept. 11, 2008, at A1; Jane Perlez, *Pakistan's Military Chief Criticizes U.S. Over a Raid*, N.Y. TIMES, Sept. 11, 2008, at A8; Eric Schmitt & Thom Shanker, *Officials Say U.S. Killed an Iraqi in Raid in Syria*, N.Y. TIMES, Oct. 28, 2008, at A1; Eric Schmitt & Mark Mazzetti, *Secret Order Lets U.S. Raid Al Qaeda*, N.Y. TIMES, Nov. 10, 2008, at A1; Ismail Khan & Jane Perlez, *Airstrike Kills Militant Tied to Al Qaeda in Pakistan*, N.Y. TIMES, Nov. 23, 2008, at A10.

When states take matters into their own hands, they tend to justify their actions under the mantle of law, even when they fail to meet the accepted legal threshold. This is done as a tactical measure to secure the broadest possible support for their actions, though at times, the states actually believe their actions are legal. Sean Murphy, *The Doctrine of Preemptive Self-Defense*, 50 VILL. L. REV. 699, 727–31 (2005).

⁵⁰ See Murphy, *supra* note 49, at 704–05.

⁵¹ Garnett & Clarke, *supra* note 13, at 488; GREENBERG ET AL., *supra* note 24, at 99–100; KAMAL, *supra* note 22, at 83–84; Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. INT'L L.J. 179, 181–83 (2006); Condrón, *supra* note 24, at 415–16; Hollis, *supra* note 22, at 1023.

can easily track attackers.⁵² Another proposal calls for a comprehensive international treaty to regulate cyberattacks.⁵³ Other scholars advocate changing the law of war to allow states to respond to cyberattacks with active defenses, without having to attribute cyberattacks to a state. Thus, one scholar proposed exempting states from having to attribute attacks against their critical infrastructure.⁵⁴ Another posited that attributing attacks is unnecessary because states can legally respond to attacks by non-state actors with force under customary international law (CIL).⁵⁵ While these approaches are all preferable to the current legal paradigm, each has its shortcomings, which this article will address.⁵⁶

The legal authority for states to use active defenses flows from states' duty to prevent non-state actors within their borders from committing cross-border attacks. "It is a long-established principle of international law that 'a state is bound to use due diligence to prevent the commission within its dominions of criminal acts against another nation or its people.'"⁵⁷ Traditionally, this duty only required states to prevent illegal acts that the state knew about beforehand; however, this duty has evolved in response to international terrorism to require states to act against groups generally known to carry out illegal acts.⁵⁸ In the realm of cyberwarfare, states must take this duty one step further by requiring states to enact and enforce criminal laws as the only way to truly prevent cross-border cyberattacks. Otherwise, the current situation that states face with China and Russia will continue to exist. While no international treaty affirmatively obligates a state to hunt down attackers within its

⁵² See generally LAWRENCE LESSIG, CODE: VERSION 2.0 (2006).

⁵³ See generally Brown, *supra* note 51, at 179.

⁵⁴ See Jensen, *supra* note 5, at 236–37; Condron, *supra* note 24, at 415–22.

⁵⁵ See Barkham, *supra* note 29, at 104; Michael Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 933–34 (1999). This proposal would allow states to use active defenses regardless of who is conducting the cyberattack.

⁵⁶ See *infra* note 168 and accompanying text (discussing the shortcomings of treaty based solutions); *infra* note 377 and accompanying text (discussing the shortcomings of the current proposals to change the law of war).

⁵⁷ Michael Schmitt, *Preemptive Strategies in International Law*, 24 MICH. J. INT'L L. 513, 540–41 (2003) (quoting S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 88 (Sept. 7, 1927) (Moore, J., dissenting), and referring to numerous state pronouncements to that effect with regard to international terrorism).

⁵⁸ See *infra* Part V.B (discussing the traditional and contemporary views of a state's duty to prevent non-state actors within their borders from committing cross-border criminal acts).

borders, such as with piracy,⁵⁹ reinterpreting the duty of prevention to require states to hunt down attackers will solve the attribution problem and response crisis. Once this duty is reinterpreted, international law allows victim-states to impute state responsibility to host-states that neglected this duty, and respond in self-defense.⁶⁰ In effect, repeated failure by a state to take criminal action against its attackers will result in it being declared a sanctuary state, allowing victim-states to use active defenses against cyberattacks originating from within its borders.

Selectively targeting sanctuary states with active defenses will likely provide the added benefit of prompting sanctuary states to take cyberattacks seriously as a criminal matter. Since no state wants another state acting within its borders, even electronically, this reinterpreted duty will motivate states to hunt down attackers within their borders and work with victim-states to bring attackers to justice. States who wish to avoid being the targets of active defenses can easily do so; all they have to do is pass stringent criminal laws, conduct vigorous and transparent criminal investigations, and prosecute attackers.⁶¹

III. Examining Cyberattacks

Effective regulation requires an understanding of the conduct it seeks to regulate. Attempting to regulate a subject without understanding it can easily lead to ineffective regulations that fail to accomplish their intended purpose. This article shall, therefore, examine cyberattacks, their potential impact, and the defenses against them, as a precursor to exploring the legal regime governing them.

A. Types of Cyberattacks

Cyberattacks come in many different forms. To generalize, there are three main categories of cyberattacks.⁶² The first category is automated

⁵⁹ See U.S. DEP'T OF NAVY, NWP 1-14M, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS § 3.5 (2007) [hereinafter COMMANDER'S HANDBOOK] (referencing international law's long-standing obligation for states to repress piracy, and quoting the 1958 Geneva Convention on the High Seas and the 1982 Law of the Sea Convention).

⁶⁰ See *infra* Part V–VI.

⁶¹ See *infra* Part VI.B–C.

⁶² Cyberattacks can be categorized in different ways. It is this author's opinion that there are three main categories of cyberattacks. However, other authors categorize

malicious software delivered over the Internet.⁶³ The second category is denial-of-service (DOS) attacks.⁶⁴ The third category is unauthorized remote intrusions into computer systems by individuals.⁶⁵

Before considering these three, it is worth noting that cyberattacks can originate locally rather than remotely over the Internet. For instance, malicious software may be locally loaded onto a system via a storage device, such as a thumb drive or computer disk, and unauthorized intrusions may originate at a physical terminal connected to a computer network. However, while computer systems are more vulnerable to penetration at their physical location, this article focuses on external cyberattacks conducted via the Internet across international borders.⁶⁶

Malicious code, or malware, usually infects computer systems through infected e-mails, vulnerability exploit engines, or visits to infected websites.⁶⁷ Early malware fell into two main classifications, viruses and worms.⁶⁸ Viruses are code fragments that copy themselves into larger programs, modifying those programs to carry out functions

cyberattacks into as little as two or as many as four main categories. *See* LEHTINEN ET AL., *supra* note 36, at 79–95, 112–33 (categorizing cyberattacks into viruses and Internet vulnerabilities); COLARIK, *supra* note 6, at 84 (categorizing cyberattacks into viruses, denial-of-service attacks, web defacements, and unauthorized penetration).

⁶³ *See* COLARIK, *supra* note 6, at 84.

⁶⁴ *See id.*

⁶⁵ *See id.*

⁶⁶ Internal penetrations are a serious issue despite not being the focus of this article. Authorized users, also known as insiders, have greater access to computer systems than unauthorized users. This access makes it easy for them to load malicious code onto a system, or to do something beyond their authorization. *See id.* at 85–86. Internal penetrations can be inadvertent or intentional. In the case of an inadvertent penetration, a user might connect an infected storage device to a computer network, which then executes its code to the detriment of the system. In the case of an intentional penetration, a user could simply use their access to conduct harmful acts within their access rights, or attempt to use their limited access to try to gain greater access to the system and then conduct harmful acts. *See* LEHTINEN ET AL., *supra* note 36, at 96–111. However despite being a cyberattack of sorts, internal penetrations should fall under domestic law, as the cyberattack occurs as a result of a physical act at the location of the computer networks. This puts internal penetrations squarely in the domestic jurisdiction of the state in question. Absent an intentional act by a member of a transnational terrorist organization, who happens to have gained local access to a computer system, there is no international character to the penetration. In the case that such an act is committed by a transnational terrorist, some of the concepts discussed in this article may be appropriate for analogy.

⁶⁷ LEHTINEN ET AL., *supra* note 36, at 79; COLARIK, *supra* note 6, at 84.

⁶⁸ LEHTINEN ET AL., *supra* note 36, at 80. These definitions were derived from the methods the programs used to carry out an attack. *Id.*

other than those originally intended.⁶⁹ The virus is dependent on the main program, and cannot execute until the main program is run.⁷⁰ Once the main program is run, viruses load themselves into the memory of the computer system and execute their code.⁷¹ A virus then replicates itself, infecting other programs and files.⁷² After it finishes reproducing, it carries out whatever dirty work is in its programming, called delivering a payload.⁷³ Worms are self-sustaining independent programs that reproduce themselves by copying themselves in full-blown fashion from one computer to another via a network or the Internet.⁷⁴ Worms can spread rapidly from system to system, copying themselves to any computer systems connected to the infected computer and, if programmed to do so, delivering their payload on the new system after replicating.⁷⁵

As computer programs became more sophisticated, the terms viruses and worms failed to adequately describe the diverse nature of malware.⁷⁶ As a result, these categories were further defined by their function.⁷⁷ The most common subdivisions of viruses and worms are Trojan horses, rootkits, sniffers, exploits, bombs, and zombies.⁷⁸ Attackers may choose

⁶⁹ *Id.* at 81–82.

⁷⁰ *Id.*

⁷¹ *Id.* at 82; COLARIK, *supra* note 6, at 91.

⁷² LEHTINEN ET AL., *supra* note 36, at 82; COLARIK, *supra* note 6, at 91–92.

⁷³ LEHTINEN ET AL., *supra* note 36, at 82.

⁷⁴ *Id.* at 85.

⁷⁵ *Id.*; COLARIK, *supra* note 6, at 92.

⁷⁶ LEHTINEN ET AL., *supra* note 36, at 80.

⁷⁷ *Id.*

⁷⁸ *Id.* at 80–81. Trojan horses trick a user into running a program that appears beneficial but actually has a code fragment hidden inside the program, which performs a disguised function. *Id.* at 87. Rootkits install new accounts on a computer system or steal existing account information, and then elevate the security level of those accounts to the highest degree so that the attacker can later enter at will without obstruction. *Id.* at 81, 87. Sniffers monitor the keystrokes of authorized users and send the stolen information back to a storage facility for later access by the program designer. *Id.* at 81, 88. Exploits are programs that capitalize on known or undiscovered system vulnerabilities, such as weaknesses in a piece of software or the operating system, to gain access to the system and execute their program. *Id.* at 81, 87. Exploits may also capitalize on system vulnerabilities created through poor security practices and procedures, in addition to those created by technical errors. See WILSON, *supra* note 15, at CRS-25. Bombs are programs that destroy data by reformatting the hard disk, or by corrupting files by inserting random data into them. U.S. ARMY TRAINING & DOCTRINE COMMAND, DCSINT HANDBOOK No. 1-02, CRITICAL INFRASTRUCTURE THREATS AND TERRORISM, at VII-7 (2006) [hereinafter CRITICAL INFRASTRUCTURE THREATS]. Bombs can execute immediately after being loaded onto a system or be delayed. LEHTINEN ET AL., *supra* note

a single one of these programs or use them in conjunction with each other.⁷⁹ Additionally, attackers may also use malware in conjunction with DOS attacks and unauthorized remote intrusions.⁸⁰

Denial-of-service attacks use computers' communication protocols against them, overwhelming the targeted computer system with information until it seizes up and cannot function.⁸¹ This effectively denies the availability of the targeted system to legitimate users.⁸² Denial-of-service attacks can use malformed packets to overwhelm a system's processors, or flood the processor with so many data requests that it overwhelms the system itself or its supporting network bandwidth.⁸³ The most severe form of DOS attack is a distributed-denial-of-service (DDOS) attack.⁸⁴ Distributed-denial-of-service attacks are DOS attacks launched simultaneously from numerous computers.⁸⁵ The sheer volume of a DDOS attack makes it extremely difficult to defend against.⁸⁶ In addition to crippling computer systems attached to the Internet, DOS attacks can overwhelm system defenses, such as

36, at 88. Time bombs can be set to go off at a specific time; logic bombs can be set to go off after a particular event occurs. *Id.* at 88. A zombie is malware that entrenches itself inside a computer system and then lays low until the attacker triggers it into action. *Id.* at 81, 83.

⁷⁹ See LEHTINEN ET AL., *supra* note 36, at 79–95. For example, an attacker may use a trojan horse to deliver a rootkit or sniffer, or he may use an exploit to implant a zombie.

⁸⁰ *Id.*

⁸¹ See *id.* at 81; COLARIK, *supra* note 6, at 84, 103.

⁸² LEHTINEN ET AL., *supra* note 36, at 12.

⁸³ See COLARIK, *supra* note 6, at 103.

⁸⁴ See *id.*

⁸⁵ LEHTINEN ET AL., *supra* note 36, at 81. Distributed-denial-of-service attacks are usually launched from zombies, which attackers hijack ahead of time. These virtual networks of zombies all being directed at once for a single nefarious purpose are known as Botnets. It is not unheard of to have several hundred thousand zombies, or Bots, harnessed at once to unleash one coordinated massive attack. Botnets can be used to deliver malicious code, gather information, or conduct DDOS attacks. See WILSON, *supra* note 15, at CRS-5 to CRS-7.

An interesting evolution of DDOS attacks occurred in 2007 with the “e-Jihad” computer program. E-Jihad let computer owners freely give control of their system to the creators of e-Jihad, who agreed to use their computers to attack anti-Islamic entities. E-Jihad would coordinate the attacks of the freely lent computers, effectively turning them into a network of zombies, and report back to the owners on the success rates of the attacks. E-Jihad has since been shut down, but there will inevitably be similar programs in the future. See Larry Greenemeier, “*Electronic Jihad*” App Offers Cyberterrorism for the Masses, INFORMATIONWEEK.COM, July 2, 2007, <http://www.informationweek.com/news/Internet/show/Article.jhtml?articleID=20000193>.

⁸⁶ See COLARIK, *supra* note 6, at 103.

knocking down a firewall, so that the system becomes vulnerable to other forms of attack.⁸⁷

Remote intrusions are external penetrations of a computer system by an attacker.⁸⁸ They occur at user access points and require user account names and passwords.⁸⁹ Attackers usually use malware to infect computer systems to acquire the necessary access or create fake user accounts on target systems. However, attackers also use social engineering, packet sniffers, and password cracking tools to acquire user account information.⁹⁰ Once an attacker gains access to a system, the attacker can do a variety of harmful things with or to the system, including “caus[ing] people or processes to act on the changed data in a way that causes a cascading series of damages in the physical and electronic world.”⁹¹

B. Potential Impact of Cyberattacks

The Internet’s open architecture makes it “ideally suited for asymmetrical warfare.”⁹² Cyberattacks “can be used by both states and non-state actors to anonymously pry into a state’s public, sensitive and classified computers . . . to manipulate data; to deceive decision makers; to influence public opinion; and even to cause physical destruction from

⁸⁷ *Id.* Web-based attacks, such as a DOS attack, can be used to cause a buffer overflow in the memory of the targeted computer. Buffer overflows of the computer’s stack—the part of memory used for temporary variable storage—can cause the computer to write the overflow of data to the computer’s heap—the segment of memory that stores code waiting for execution. This is called “smashing the stack.” Smashing the stack allows attackers to implant executable programs into the targeted computer to gain further access. Imagine a rootkit being implanted this way. *See* LEHTINEN ET AL., *supra* note 36, at 131–32.

⁸⁸ *See* COLARIK, *supra* note 6, at 94.

⁸⁹ *See id.* at 97.

⁹⁰ *See id.* at 97–98. Social engineering tricks users into giving away their account information. This often happens when attackers impersonate company employees or system administrators over the phone. *Id.* at 94. Packet sniffers capture user data being transmitted to or from a system. *Id.* at 97–98. Password cracking comes in two forms, brute force and dictionary attacks. Brute force attacks guess passwords “by trying every possible combination of characters, one attempt at a time.” Dictionary attacks guess passwords by using commonly used words or variations thereof. Dictionary attacks are often aided by advance reconnaissance, as many people pick easy passwords, such as their initials or children’s names. LEHTINEN ET AL., *supra* note 36, at 61.

⁹¹ COLARIK, *supra* note 6, at 84.

⁹² WINGFIELD, *supra* note 48, at 21.

remote locations abroad.”⁹³ Cyberattacks overcome the requirement for conventional military forces, allowing attackers who understand computer systems to inflict damage on another state, anonymously and for minimal cost, from the other side of the globe.⁹⁴

Attackers can direct cyberattacks at any computer system connected to the Internet; however, the most dangerous attacks are those against critical national infrastructure (CNI).⁹⁵ These systems are so essential to a state’s well-being that states have sworn to protect them regardless of whether the systems are civilian or governmental.⁹⁶ While there is no inclusive list of CNI, a functional analysis of the role that computers play in key resource sectors shows that computer systems form the backbone of almost every nationally significant sector, including banking and finance, communications, energy, emergency services, government, transportation, and water supply.⁹⁷ Cyberattacks against these sectors can intimidate populations, damage an economy, and even injure or kill.⁹⁸ Furthermore, cyberattacks provide terrorists a way to increase the destructive impact of physical attacks.⁹⁹ In essence, cyberattacks are just another tool for a state’s enemies to use.

Cyberattacks, like conventional terrorist attacks, can terrorize a population. The National Security Agency has demonstrated that cyberattacks can disrupt operations at major military commands, cause

⁹³ *Id.* at 21–22.

⁹⁴ *See id.* at 22.

⁹⁵ *See* Timothy Shimeall et al., *Countering Cyber War*, 49 *NATO REV.* 16, 17–18 (Winter 2001/2002), available at <http://www.nato.int/docu/rev-pdf/eng/0104-en.pdf> (noting cyberattacks on CNI would likely result in significant loss of life, and economic and social degradation). While cyberattacks against CNI are the most dangerous form of cyberattack, lesser attacks are still destructive. For instance, the FBI recently estimated that cybercrime, a subset of cyberattacks, causes an average financial loss of \$167,713 per attack, and as a whole has caused over \$400 billion in damages in the United States. WILSON, *supra* note 15, at CRS-27 to CRS-29.

⁹⁶ *See* Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection (2003); Condon, *supra* note 24, at 404–07; Jensen, *supra* note 5, at 226–28; JOHN MOTEFF, CONG. RESEARCH SERV. REPORT, CRITICAL INFRASTRUCTURES: BACKGROUND, POLICY, AND IMPLEMENTATION, RL 30153, at CRS-3 to CRS-13 (2008).

⁹⁷ *See generally* Department of Homeland Security, Critical Infrastructure and Key Resources, http://www.dhs.gov/xprevprot/programs/gc_1189168948944.shtm (last visited Mar. 22, 2009) (detailing the different sectors of critical national infrastructure and explaining their interrelations).

⁹⁸ *See* COLARIK, *supra* note 6, at 15–28 (2006).

⁹⁹ *See id.* at 51–52; WILSON, *supra* note 15, at CRS-21.

large-scale blackouts, and interrupt phone service across the United States.¹⁰⁰ Furthermore, much of the United States' CNI is controlled by Supervisory Control and Data Acquisition (SCADA) systems, which are particularly vulnerable to cyberattacks.¹⁰¹ When cyberattacks shut down these systems, people, businesses, and governments can be deprived of basic services. This can cause panic in a populace, effectively turning these cyberattacks into a means of scaring a population, potentially for political ends.¹⁰² Another vulnerability of corporate, government, and military critical systems is their frequent reliance on commercial-off-the-shelf (COTS) hardware and software.¹⁰³ Systems relying on COTS products are more vulnerable to penetration than specially designed systems, making them easier to exploit, more susceptible to damage, and thus more likely to lead to harm to a state and its citizens.¹⁰⁴ Intimidating populations with cyberattacks is just another way for terrorists to sow fear.

The potential economic consequences of cyberattacks are just as profound. Cyberattacks have the potential to cripple a state's commercial infrastructure, such as a stock exchange, and bring the state's economy to its knees.¹⁰⁵ Cyberattacks on the underlying economic infrastructure of a state are an attractive method of warfare for terrorists because so much of a state's economy is facilitated by

¹⁰⁰ See WINGFIELD, *supra* note 48, at 24–25 (discussing the 1997 *Eligible Receiver* military exercise).

¹⁰¹ WILSON, *supra* note 15, at CRS-21 to CRS-23. Supervisory control and data acquisition systems are often remotely located and unmanned, but still connected to the Internet to perform their command and control functions. *Id.* They are used to manage public and private utilities, and much of the communications infrastructure. COLARIK, *supra* note 6, at 122.

¹⁰² See COLARIK, *supra* note 6, at 19–20, 118–24 (2006). The vulnerability of SCADA systems has been demonstrated many times. In 2003, the “Slammer” worm shut down the control systems of an Ohio nuclear power plant. WILSON, *supra* note 15, at CRS-22. Also in 2003, the “Blaster” worm interrupted the warning systems of the northeastern power grid and contributed to the 2003 blackout across the eastern United States. *Id.* at CRS-23. In 2007, the Aurora Generator Test conducted by Idaho National Laboratories demonstrated that coordinated cyberattacks can overheat and shut down power turbine generators. *Id.* at CRS-19 to CRS-20. Furthermore, security experts believe that Chinese cyberattacks contributed to two blackouts in the United States. The first was the northeastern blackout in 2003; the second was the Daytona Beach and Monroe County, Florida blackout in February 2008. Shane Harris, *China's Cyber-Militia*, NAT'L J., May 31, 2008, cover story.

¹⁰³ WILSON, *supra* note 15, at CRS-23 to CRS-24; COLARIK, *supra* note 6, at 130.

¹⁰⁴ WILSON, *supra* note 15, at CRS-24. Government use of COTS systems have already resulted in the infiltration of top-secret computer systems on more than one occasion. *Id.*

¹⁰⁵ WINGFIELD, *supra* note 48, at 24–25; COLARIK, *supra* note 6, at 139.

telecommunications and computer systems.¹⁰⁶ Successful terrorist attacks on banking and finance CNI have the potential to undermine confidence in a state's economic infrastructure and increase the costs of doing business to the point of becoming commercially infeasible.¹⁰⁷ At a time when tens of trillions of dollars are held by international banks, worldwide annual credit card purchases nearly reach two trillion dollars, and online sales in the United States already amount to hundreds of billions per annum, cyberattacks provide an extremely attractive attack method for a state's enemies.¹⁰⁸

Cyberattacks also have the potential to injure or kill, either directly or indirectly.¹⁰⁹ Cyberattacks directed against the transportation sector, for example, could crash airplanes¹¹⁰ or cause trains to collide.¹¹¹ The transportation sector relies heavily on SCADA and COTS systems, and has already proven vulnerable to cyberattacks.¹¹² Cyberattacks could also be directed against dams, causing floodgates to open,¹¹³ or chemical, nuclear, and liquid natural gas plant control systems, which could easily lead to widespread physical damage or death.¹¹⁴ To illustrate these points, in 2000 a cyberattack took control of a sewage plant in Maroochy Shire, Australia, and dumped 264,000 gallons of untreated sewage into the local environment.¹¹⁵ Cyberattacks could also directly target medical systems, altering critical medical information, such as blood types, immunization histories, allergies, or other critical data.¹¹⁶ "The

¹⁰⁶ See COLARIK, *supra* note 6, at 124–28.

¹⁰⁷ See *id.* at 22.

¹⁰⁸ See *id.* at 124–28 (reviewing commerce over the Internet); WILSON, *supra* note 15, at CRS-21 (referencing Chinese military journals, which claim the ability to bring down U.S. financial markets with cyberattacks); U.S. Census Bureau, The 2009 Statistical Abstract: Online Retail Sales, http://www.census.gov/compendia/statab/cats/wholesale_retail_trade/online_retail_sales.html (recording \$128.1 billion in online sales in 2007 and projecting online sales to rise to \$147.6 billion in 2008, in the Online Retail Spending report).

¹⁰⁹ See CRITICAL INFRASTRUCTURE THREATS, *supra* note 78, at VII-7.

¹¹⁰ See COLARIK, *supra* note 6, at 128–30.

¹¹¹ See CRITICAL INFRASTRUCTURE THREATS, *supra* note 78, at VII-1 (noting the railroad signal and switching system could be manipulated to cause trains to crash into each other).

¹¹² While no one was hurt when it happened, hackers have previously taken over and shut off a regional airport's control tower and runway lights. COLARIK, *supra* note 6, at 130.

¹¹³ See WILSON, *supra* note 15, at CRS-21.

¹¹⁴ SHEA, *supra* note 13, at CRS-8.

¹¹⁵ *Id.* at CRS-7.

¹¹⁶ COLARIK, *supra* note 6, at 131.

modification of such details could cause the medical practitioners to diagnose a course of treatment that could be fatal to the patient.”¹¹⁷

The scenario that concerns experts the most, however, is the use of cyberattacks against electronic emergency warning and response systems in conjunction with physical attacks.¹¹⁸ When attackers use cyberattacks to degrade state defenses to physical attacks in this manner, they exponentially amplify the likely total damage from a physical attack.¹¹⁹ Given the devastating impact that cyberattacks can have on a population’s sense of security, economic well-being, and safety, it is imperative for states to defend themselves with the best computer defenses allowed under the law.

C. Defenses Against Cyberattacks

Today, computer security is typically divided into four general categories: system access controls, data access controls, security administration, and secure system design.¹²⁰ These defenses function on the general axiom of computer security that states can limit the damage from cyberattacks by reducing an attacker’s ability to gain unauthorized access to a computer system.¹²¹ The more secure a system is designed, the more difficult it is for attackers to penetrate the system and cause harm.¹²²

Computer security has a potential fifth category: active defenses.¹²³ Passive defenses differ from active defenses in that they do not use force, and as a result, are considered lawful under international law.¹²⁴ Active defenses, on the other hand, employ electronic force to counterattack the

¹¹⁷ *Id.*

¹¹⁸ SHEA, *supra* note 13, at CRS-9.

¹¹⁹ COLARIK, *supra* note 6, at 138–40; CRITICAL INFRASTRUCTURE THREATS, *supra* note 78, at VII-7; SHEA, *supra* note 13, at CRS-9. Furthermore, evidence indicates that terrorists are conducting cybersurveillance on U.S. critical infrastructure for this purpose. SHEA, *supra* note 13, at CRS-6 to CRS-7.

¹²⁰ LEHTINEN ET AL., *supra* note 36, at 49–50.

¹²¹ *See* COLARIK, *supra* note 6, at 83 (noting that without access, all an attacker can do is shut down a system or prevent access to it).

¹²² *See* LEHTINEN ET AL., *supra* note 36, at 49 (noting that computer security makes sure computers do what they are supposed to do by protecting the data stored in a computer from being read, destroyed, or modified by those without authorized access).

¹²³ *See* Jensen, *supra* note 5, at 230.

¹²⁴ *Id.*

source of a cyberattack, and may only be used when force is authorized under the law of war.¹²⁵ So far, states have confined their computer security to passive defenses, as active defenses are forbidden under the prevailing view of the law of war.¹²⁶ However, all five categories of computer security provide states with essential tools to protect themselves from cyberattacks.

The first form of passive defenses are system access controls. They prevent unauthorized users from getting into a system, and force authorized users to be security conscious.¹²⁷ System access controls start with identification and authentication.¹²⁸ This may be as simple as providing a username and password,¹²⁹ or it may require technological devices to login, such as an electronic key, token, badge, or smart card.¹³⁰ Some systems are so advanced that biometric or behavioral information is required to access them, such as fingerprints, handprints, retina pattern, iris pattern, voice, signature, or keystroke patterns.¹³¹ Other system access controls include transmission encryption,¹³² challenge and response procedures,¹³³ and password controls.¹³⁴

¹²⁵ *Id.* at 231.

¹²⁶ *See supra* Part II.A.

¹²⁷ LEHTINEN ET AL., *supra* note 36, at 49.

¹²⁸ Identification is how users tell the system who they are. Authentication is how users prove to a system they are who they say they are. *Id.* at 50–51.

¹²⁹ *Id.* at 51.

¹³⁰ These devices contain electronic code that allows access a system, and may even be so sophisticated as to continually calculate new passwords based on time of day or secure algorithms. The computer system being accessed will have matching information to the security device, and will grant access once the petitioning party's password matches. *Id.*

¹³¹ *Id.*

¹³² LEHTINEN ET AL., *supra* note 36, at 52. Encryption scrambles data during transmission, which can only be unlocked with the correct session key. Numerous encryption protocols can be used, such as DES, Kerberos, and Rijndael, all of which use some version of session keys to authenticate messages and protect communications. *See* LEHTINEN ET AL., *supra* note 36, at 137–72; COLARIK, *supra* note 6, at 72–73.

¹³³ Challenge and response is a protocol where users are asked to re-authenticate themselves frequently at random intervals throughout their session with the system. LEHTINEN ET AL., *supra* note 36, at 52.

¹³⁴ Password controls may attempt to stop unauthorized users from accessing a system. These controls include warning messages to unauthorized users, limiting the number of attempts to enter the correct password, implementing login failure wait times between attempts, and password locks for incorrect logins. Password controls may also force users to be more security conscious. These controls may force users to change their password at regular intervals, have minimum length passwords, and read the date/time of their last login. *Id.* at 59–60.

Data access controls are similar to system access controls, except that instead of protecting the system at-large, their protection is aimed at the data and programs inside the system.¹³⁵ Authorization is the key to data access controls. It checks to see if the users of a system have rights to access particular files.¹³⁶ Data access controls allow multiple users to use a system without having to grant everyone access to every file on the system.¹³⁷ Other data access controls include data storage encryption¹³⁸ and reference monitors.¹³⁹

Security administration is the human side of computer security.¹⁴⁰ It uses security procedures to protect a system, delineates system administrator responsibilities, ensures users are trained on computer security, and monitors users to ensure security policies are observed.¹⁴¹ Examples of security administration are setting and publicizing security policies,¹⁴² performing risk analysis and disaster planning,¹⁴³ training and monitoring employees,¹⁴⁴ creating and maintaining user security profiles,¹⁴⁵ penetration testing,¹⁴⁶ backing up system files,¹⁴⁷ arranging

¹³⁵ *Id.* at 50.

¹³⁶ Systems typically maintain a file containing information about user privileges and characteristics. This is often called a security profile. *Id.* at 61–62.

¹³⁷ See LEHTINEN ET AL., *supra* note 36, at 61–67; COLARIK, *supra* note 6, at 69–71. This is another important layer of security on top of system access controls, as it helps stop attackers from accessing sensitive data or programs after they have gained unauthorized access to a system. LEHTINEN ET AL., *supra* note 36, at 66.

¹³⁸ Encryption of stored data helps prevent the access of and tampering with sensitive information. COLARIK, *supra* note 6, at 71.

¹³⁹ Reference monitors review access attempts and cross-reference them against user security profiles. If a user attempts to access files above their access level, then the reference monitor alerts the system administrator. *Id.*

¹⁴⁰ LEHTINEN ET AL., *supra* note 36, at 96.

¹⁴¹ *Id.* at 50.

¹⁴² Security policies are designed to make systems more secure. An example of a security policy is the separation of administrator duties. The separation of duties prevents any one user from controlling the system's security mechanisms. By separating duties among a group of individuals, it becomes harder for cyberattackers to take control of a system through the impersonation of an individual account. *Id.* at 97, 108–10.

¹⁴³ *Id.* at 97.

¹⁴⁴ *Id.*

¹⁴⁵ *Id.* at 97.

¹⁴⁶ Penetration testing is when the system administrator simulates cyberattacks to test a computer system for security holes. *Id.* at 97, 107–08.

¹⁴⁷ Backing up data may occur on site or at remote secure facilities, and is one of the most important things a system administrator can do to enable a compromised system to recover from a cyberattack. *Id.* at 96, 102.

for the use of other computer facilities or equipment in case of an emergency,¹⁴⁸ and performing security audits.¹⁴⁹

Secure system design uses hardware and software to protect the system.¹⁵⁰ Examples of security hardware are segmented system memory¹⁵¹ and physical gateways.¹⁵² In addition, a system can be built to withstand denial-of-service attacks.¹⁵³ Examples of security software are anti-virus programs,¹⁵⁴ encryption programs, firewalls,¹⁵⁵ and intrusion detection systems.¹⁵⁶

¹⁴⁸ Backup systems may be essential in case a cyberattack cripples an organization's primary systems. *Id.* at 96.

¹⁴⁹ Security audits review user profiles and activity within a system and look for suspicious account settings or activity. An effective component of a security audit is to review audit logs/trails. Audit logs/trails are designed to record activities and events within a computer system. Reviewing audit logs/trails can reveal security breaches inside a system and help trace the attacks back to their source. For instance, an audit log might contain information about the origin of a computer transmission, show which files were accessed or attempted to be accessed, and reveal changes to the computer system. *Id.* at 108–09; COLARIK, *supra* note 6, at 71–72 (2006).

¹⁵⁰ LEHTINEN ET AL., *supra* note 36, at 50.

¹⁵¹ Segmented system memory physically isolates privileged processes from non-privileged processes. *Id.*

¹⁵² The easiest way to secure a computer network is to physically isolate it from the outside world. However, as systems become increasingly dependent on global communication to achieve its purpose, this becomes more difficult to do. There is a middle ground, though. Systems can be physically designed so that communication to and from the system are routed through a single channel, known as a gateway. Gateways can be designed to run a variety of security programs, all aimed at ensuring that communication is coming from trusted sources for legitimate purposes. *Id.* at 189.

¹⁵³ This can include increasing bandwidth to handle the scope of the attack, building redundant or fault-tolerant systems that are harder to disrupt, or building the network so that it is easy to reconfigure in case of attack. *See id.* at 196.

¹⁵⁴ Anti-virus programs contain registries of virus code patterns that can be used to detect viruses. Anti-virus programs lurk in the background of computer systems, constantly running and scanning ongoing processes and incoming data for viral code. Upon detecting a potential virus, the program sounds an alarm and attempts to quarantine the dangerous code. *Id.* at 92–93.

¹⁵⁵

[F]irewalls protect[] [computer systems] by examining each packet [of data] that travels over the network. Clues about a packet's purpose can be read from its destination address. Firewalls contain a list of allowed and disallowed destinations and functions. If a packet is heading for a forbidden address or comes from one, the firewall stops it. If a packet is heading for a valid address, but its port identifier (the clue to packet function) is unknown or disallowed, the firewall stops that packet as well. Advanced firewalls even keep track of outgoing packets, and open up only if a packet is expected and returning.

Active defenses involve an in-kind response to a cyberattack—effectively, a counter-cyberattack against the attacker’s system, shutting down the attack before it can do further harm and/or damaging the perpetrator’s system to stop it from launching future attacks.¹⁵⁷ Security professionals can set up active defenses to automatically respond to attacks against critical systems or can carry them out manually.¹⁵⁸ For the most part, active defenses are classified, though programs that send destructive viruses back to the perpetrator’s machine or packet-flood the intruder’s machine have entered the public domain.¹⁵⁹ The specific capabilities that the Government has developed are beyond the scope of this article; however, it is essential to note that active defenses greatly enhance a victim-state’s defensive capabilities against cyberattacks by providing it with a crucial additional option over passive defenses alone.¹⁶⁰

Defending against cyberattacks goes beyond computer security. On the macro level in the United States, “the federal government has taken steps to . . . encourage the private sector to also adopt stronger computer security policies and practices to reduce infrastructure vulnerabilities.”¹⁶¹ The National Strategy to Secure Cyberspace encourages the private sector to partner with federal agencies to improve computer security for U.S. critical infrastructure.¹⁶² The National Cyber Security Division of the Department of Homeland Security is “tasked with conducting analysis of cyberspace threats and vulnerabilities, issuing alerts and

Firewalls help prevent active threats such as worms and viruses, which attempt to enter a computer via forbidden pathways. *Id.* at 92.

¹⁵⁶ Intrusion detection systems monitor systems for attacks, much like anti-virus programs do for viruses. The intrusion detection systems have libraries of the steps that attackers typically take to conduct attacks. If an attack pattern is identified, it tries to stop the transaction (if it can) and places a call to the system administrator, informing them of the attempted attack. *Id.* at 107.

¹⁵⁷ See Jensen, *supra* note 5, at 231; Condrón, *supra* note 24, at 410–11.

¹⁵⁸ See Jensen, *supra* note 5, at 231; David Wheeler & Gregory Larsen, *Techniques for Cyber Attack Attribution*, INST. DEF. ANALYSIS, Oct. 2003, at 23–24, available at <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468859&Location=U2&doc=GetTRDoc.pdf>.

¹⁵⁹ See Jensen, *supra* note 5, at 231; Condrón, *supra* note 24, at 410–11.

¹⁶⁰ See Shachtman, *supra* note 25 (quoting the Air Force Research Laboratory as saying that passive defenses are insufficient to stop cyberattacks, and that active defenses are needed to mount an effective defense against cyberattacks); Crovitz, *supra* note 14, at 17 (arguing active defenses are needed to stop the cyberthreat).

¹⁶¹ WILSON, *supra* note 15, at CRS-31.

¹⁶² *Id.*

warnings for cyberthreats, improving information sharing, responding to major cybersecurity incidents, and aiding in national-level recovery efforts.”¹⁶³ Furthermore, the Government has set up the Cyber Warning and Information Network and National Cyber Alert System, which is an early warning system for cyberattacks across the United States that coordinates national cybersecurity defenses across critical U.S. sectors.¹⁶⁴

Unfortunately, computer security in its present form is not enough to stop cyberattacks. Computer software frequently has design flaws that open systems to attack, despite system administrators’ best efforts to fully secure their computer systems.¹⁶⁵ These design flaws are compounded by administrator and user carelessness in both system design and use, which often nullify the security measures put in place to defend a system.¹⁶⁶ Furthermore, poor design of federal computer networks has left them with more entry points than U.S. early warning programs can effectively monitor at one time, leaving U.S. computer systems vulnerable to attack until the amount of entry points is reduced.¹⁶⁷ These vulnerabilities highlight the fact that passive defenses alone are not enough to protect states from cyberattacks. As a result, it is likely that states will feel the need to use active defenses. In such event, it would be best if international law could provide parameters regarding their proper use.¹⁶⁸

¹⁶³ *Id.*

¹⁶⁴ *Id.* at CRS-31 to CRS-32.

¹⁶⁵ *See id.* at CRS-24 to CRS-26.

¹⁶⁶ *See* LEHTINEN ET AL., *supra* note 36, at 96; WILSON, *supra* note 15, at CRS-25.

¹⁶⁷ *See* Ryan Naraine, *Chertoff Describes “Manhattan Project” for Cyber Defenses*, EWEEK.COM, Apr. 8, 2008, <http://www.eweek.com/c/a/Security/Chertoff-Describes-Manhattan-Project-for-Cyber-Defenses> (referencing former Secretary of Homeland Security Michael Chertoff’s speech on federal computer systems’ vulnerability).

¹⁶⁸ There are three different ways for international law to deal with cyberattacks. First, international law can continue to force states to deal with cyberattacks as a criminal matter. However, not only does this option fail to provide any guidance on the use of active defenses, but it continues to leave states vulnerable to cyberattacks. *See supra* Part II.A.

Second, states can amend international law through international treaties to provide new ways to combat cyberattacks. These treaties could either regulate state responsibilities concerning international cyberattacks or regulate the architecture and code used to build the Internet. *See generally* Brown, *supra* note 51 (discussing the importance of an international convention on cyberattacks); LESSIG, *supra* note 52 (arguing for an international treaty to regulate the design of cyberspace to make it easier for law enforcement to trace attacks and prosecute attackers). However, since meaningful international agreements require the agreement of a substantial majority of sovereign states, it seems unlikely that any comprehensive treaty will be forthcoming in the near future. *See* LESSIG, *supra* note 52, at 298–324. Furthermore, it is naïve to think

IV. The General Framework of *Jus ad Bellum*

The law of war is divided into two principal areas, *jus ad bellum* and *jus in bello*.¹⁶⁹ *Jus ad bellum*, also known as the law of conflict management, is the legal regime governing the transition from peace to war.¹⁷⁰ *Jus in bello*, also known as the law of armed conflict, governs the actual use of force during war.¹⁷¹ The analysis of whether states can respond to cyberattacks with active defenses predominantly falls under *jus ad bellum*, which provides (1) the thresholds that cyberattacks must cross to be considered a use of force, which would then bring cyberattacks under the *jus in bello*, and (2) the legal options that states have to respond to cyberattacks.

Historically, the transition from peace to war fell under the prerogative of the sovereign; however, it came under international law following World War II with the ratification of the U.N. Charter.¹⁷² While the U.N. Charter is not the only source of *jus ad bellum*,¹⁷³ it has redefined and codified “contemporary *jus ad bellum* in its entirety” and has become the starting point for all *jus ad bellum* analyses.¹⁷⁴ The relevant articles of the U.N. Charter are Articles 2(4), 39 and 51, which provide the framework for modern *jus ad bellum* analyses.¹⁷⁵

that treaties will motivate states to cooperate, as states like China and Russia already turn a blind eye to cyberattacks despite international condemnation of their practices, and numerous U.N. General Assembly resolutions calling for state cooperation. *See supra* Part II.A (discussing China and Russia’s unwillingness to investigate and prosecute attackers); *infra* Part VI.C (discussing U.N. General Assembly resolutions calling for international cooperation to eradicate cyberattacks).

Finally, states can try to find a way around the legal crisis under the law of war, so that they can employ active defenses in addition to passive defenses. Of these options, finding a way to authorize active defenses under the law of war is the only realistic way to protect states from cyberattacks. The first two options require state cooperation, which is not happening at present and seems unlikely to happen in the near future.

¹⁶⁹ WINGFIELD, *supra* note 48, at 31.

¹⁷⁰ *Jus ad bellum* “is a set of rules that govern the resort to armed conflict and determine whether the conflict is lawful or unlawful in its inception.” *Id.* at 33. It governs what amounts to a use of force, and when force is authorized. *Id.* at 31, 33.

¹⁷¹ *Jus in bello* “governs the behavior of both belligerents and neutrals during hostilities.” It governs what types of force are authorized during hostilities and places limits on the use of force. *Id.* at 131.

¹⁷² *Id.* at 31.

¹⁷³ *See* Hollis, *supra* note 22, at 1039 (noting that *jus ad bellum* comes from diverse sources, including the U.N. Charter, international humanitarian law treaties, and customary international law (CIL)).

¹⁷⁴ WINGFIELD, *supra* note 48, at 31, 37–38.

¹⁷⁵ *Id.* at 31, 37–40.

A. General Prohibition on the Use of Force

Article 2(4) prohibits states from employing “the threat or use of force against the territorial integrity or political independence of [another] state, or in any other manner inconsistent with the Purposes of the United Nations.”¹⁷⁶ Sometimes known as *jus contra bellum*,¹⁷⁷ Article 2(4) criminalizes both the aggressive use of force and the threat of the aggressive use of force by states as crimes against international peace and security.¹⁷⁸ Although the U.N. Charter’s protections apply only to those states that are parties to it, the prohibitions contained in Article 2(4) have come to be recognized as CIL, binding on all states across the globe.¹⁷⁹

On its face, Article 2(4) might suggest that the threat or use of force is prohibited only when directed against the territorial integrity or political independence of another state.¹⁸⁰ This is not the case.¹⁸¹ Article 2(4) also prohibits any threat or use of force inconsistent with the purpose of the United Nations.¹⁸² When read in conjunction with Article 1 of the U.N. Charter, Article 2(4) forbids threats or uses of force that threaten international peace and security.¹⁸³ Thus, states may not threaten to use or actually use force against another state unless an exception is carved out within the U.N. Charter.¹⁸⁴ This position is further supported by Article 2(3), which requires states to “settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.”¹⁸⁵ Only two exceptions exist to this seemingly all-encompassing

¹⁷⁶ U.N. Charter art. 2(4).

¹⁷⁷ *Jus contra bellum* means the law against the aggressive use of force. WINGFIELD, *supra* note 48, at 38.

¹⁷⁸ *Id.* at 31, 38–39.

¹⁷⁹ Schmitt, *supra* note 57, at 521. Unlike treaty-based law, which only binds parties to the treaty, CIL binds all states to it. Customary international law is formed when state practice matures to the point that it evidences *opinio juris sive necessitates*, a belief on the part of states that engaging in that practice is legally obligatory. *Id.* at 524; *see infra* notes 380–81 and accompanying text (discussing the formation of CIL in depth).

¹⁸⁰ *Id.* at 521–22.

¹⁸¹ *Id.*

¹⁸² U.N. Charter art. 2(4).

¹⁸³ *See id.* art. 1 (stating that the purpose of the United Nations is to maintain international peace and security); Schmitt, *supra* note 57, at 522.

¹⁸⁴ YORAM DINSTEIN, *WAR, AGGRESSION AND SELF-DEFENCE* 87–88 (4th ed. 2005).

¹⁸⁵ U.N. Charter art. 2(3).

renunciation on the use of force:¹⁸⁶ actions authorized by the U.N. Security Council¹⁸⁷ and self-defense.¹⁸⁸

B. Actions Authorized by the U.N. Security Council

The first exception to the general prohibition on the use of force is actions authorized by the U.N. Security Council. This coercive authority stems from Article 42 of the U.N. Charter, which allows the Security Council to use military force to restore international peace and security.¹⁸⁹ However, while the U.N. Charter grants the Security Council power to use military force, the Security Council cannot do so until it has met certain conditions laid out in Articles 39, 41, and 42.¹⁹⁰

Article 39 is the first threshold that the Security Council must cross before it can authorize the use of force.¹⁹¹ The Security Council must consider whether a “threat to the peace, breach of the peace, or act of aggression” exists.¹⁹² Should the Security Council determine that this threshold has been met, in essence determining that a state has violated its obligations under Article 2(4), the Security Council may then move on to Articles 41 and 42 to determine the appropriate course of action to restore international peace and security.¹⁹³

¹⁸⁶ Jensen, *supra* note 5, at 216.

¹⁸⁷ See U.N. Charter art. 39 (stating that the Security Council shall decide what constitutes a threat to international peace and security, and what measures to take in response to any such threat); *id.* art. 42 (granting the Security Council the power to use military measures to restore international peace and security).

¹⁸⁸ See *id.* art. 51 (re-affirming the inherent right of states to use force in self-defense under CIL).

¹⁸⁹ *Id.* art. 42.

¹⁹⁰ WINGFIELD, *supra* note 48, at 31, 52–54.

¹⁹¹ U.N. Charter art. 39.

¹⁹² *Id.*

¹⁹³ See *id.* arts. 2(4), 39. Remember, states are generally prohibited from threatening to use or using force, and are required to seek peaceful means to resolve their disputes. See *id.* arts. 2(3), 2(4). Fortunately, the drafters of the Charter understood that some states would not live up to these requirements and created a framework to deal with them. “As an exercise of the international community’s inherent right of collective self-defense, Article 39 of the Charter imposes an obligation on the Security Council to maintain international peace and security.” WINGFIELD, *supra* note 48, at 52. From this obligation, and through the mechanisms prescribed by Articles 41 and 42, the Security Council derives the power to authorize the force against states who threaten the peace. *Id.* at 52–54.

Article 41, the use of non-military measures, is the Charter's preferred method for restoring international peace and security.¹⁹⁴ Under it, the Security Council may authorize non-military measures to coerce an offending state into ceasing its aggression.¹⁹⁵ The non-military measures are implemented by U.N. member states and may include the "complete or partial interruption of economic relations . . . and other means of communication, and the severance of diplomatic relations."¹⁹⁶

Like Article 41, the use of military measures under Article 42 requires an Article 39 threshold decision to be made, and only then used after non-military measures have proven unsuccessful or after the Security Council determines that it would be fruitless to adopt them.¹⁹⁷ However, unlike its Article 41 powers, the Security Council may only authorize member states to take military action; it cannot compel them to do so.¹⁹⁸

C. Self-Defense

The second exception to the general prohibition on the use of force is self-defense. This defensive right of states is enshrined in Article 51 of the U.N. Charter, which proclaims that "[n]othing in the present Charter shall impair the inherent right of [states to engage in] individual or collective self-defense" in response to an "armed attack."¹⁹⁹ As the text of Article 51 implies, the right of self-defense existed long before the

¹⁹⁴ See Schmitt, *supra* note 57, at 525.

¹⁹⁵ See *id.*

¹⁹⁶ U.N. Charter art. 41. Article 41 explicitly recognizes the Security Council's authority to give orders to Member states. WINGFIELD, *supra* note 48, at 53–54. "The Members of the United Nations agree to accept and carry out the decisions of the Security Council in accordance with the present Charter." U.N. Charter art. 25.

¹⁹⁷ See U.N. Charter art. 42; Schmitt, *supra* note 57, at 525.

¹⁹⁸ WINGFIELD, *supra* note 48, at 54. When the Security Council authorizes the use of force against a state under Article 42, its authorizing resolution serves as legal authority. The Security Council can authorize states to use military force in three different ways. First, it can authorize states to use force to enforce its resolution. Second, it can authorize international organizations, such as NATO, to use force on its behalf. Third, it can create a U.N. military force and ask states to provide military forces to it. In all of the cases, state participation is strictly voluntary and cannot be compelled. SCHMITT, *supra* note 57, at 525–28.

¹⁹⁹ U.N. Charter art. 51. Article 51 only allows states to act in self-defense until the Security Council takes action to restore international peace and security. Furthermore, states are required to immediately report measures taken in self-defense to the Security Council. *Id.*; DINSTEIN, *supra* note 184, at 177 (quoting Article 51 of the U.N. Charter).

U.N. Charter and has been re-affirmed in the Charter as an inherent right of states under CIL.²⁰⁰ Self-defense is derived from the fundamental right of states to survive, allowing them the self-help measure of using force defensively to protect themselves and their citizens.²⁰¹ Since this right exists independent of and has not been subsumed by the U.N. Charter,²⁰² self-defense analysis draws on both the provisions of Article 51 of the U.N. Charter and the principles of CIL.²⁰³

The bedrock principle of self-defense is that it may be invoked in response to an armed attack.²⁰⁴ Unfortunately, while this cornerstone is universally recognized under international law, ambiguity in the U.N. Charter has led to an ongoing debate about when states may invoke self-defense.²⁰⁵ This is because the Charter never defines “armed attack.”²⁰⁶ Since the timing of self-defense is contingent on when an armed attack occurs, it is critical to resolve what constitutes an armed attack.²⁰⁷ This debate has become even more pronounced regarding cyberattacks, which are often seen as a use of force short of armed force, making cyberattacks far more difficult to classify than traditional attacks with conventional weapons.²⁰⁸

Self-defense analysis is further complicated because of competing theories among legal scholars on the interplay between the U.N. Charter

²⁰⁰ See DINSTEIN, *supra* note 184, at 175–82.

²⁰¹ *Id.* at 175–76.

²⁰² See *Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.)*, 1986 I.C.J. 14, 94, 96–97 (June 27) (noting that the inherent right of self-defense has not been subsumed by the U.N. Charter); DINSTEIN, *supra* note 184, at 181 (citing the International Court of Justice’s (ICJ) opinion in the *Nicaragua* case); Jensen, *supra* note 5, at 221 (citing the ICJ’s opinion in the *Nicaragua* case). *But see* WINGFIELD, *supra* note 48, at 41 (citing THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 666 (Bruce Simma ed. 1994), which concludes that Article 51 excludes any right of self-defense “other than that in response to an armed attack”).

²⁰³ See DINSTEIN, *supra* note 184, at 181; WINGFIELD, *supra* note 48, at 41 (noting that the Article 51 right of self-defense is coextensive with the right of self defense under CIL).

²⁰⁴ U.N. Charter art. 51.

²⁰⁵ Hollis, *supra* note 22, at 1040–41.

²⁰⁶ See WINGFIELD, *supra* note 48, at 73; Hollis, *supra* note 22, at 1040–41.

²⁰⁷ See WINGFIELD, *supra* note 48, at 41 (noting that the pivotal focal point in any self-defense debate is the meaning of an armed attack, since that will determine the time that an armed attack occurs and when self-defense may be invoked); Jensen, *supra* note 5, at 219–20.

²⁰⁸ See *infra* Part VI.A (addressing the question of whether a cyberattack constitutes an armed attack).

and CIL.²⁰⁹ Some commentators place heavier emphasis on the U.N. Charter, arguing that Article 51 limits self-defense to responses against actual armed attacks.²¹⁰ Others place more emphasis on CIL, arguing for a broader interpretation of armed attacks that includes imminent armed attacks.²¹¹ Imminent armed attacks are addressed in Part IV, Section D. For now, it is worth noting that while there are different theories about the definition of an armed attack, once a state is targeted with an armed attack, the state and its allies are legally authorized to use force against the aggressor.

Self-defense responses must comply with international law. Just because an armed attack has occurred against a victim-state does not mean that the victim-state has a blank check to wage unlimited war against an aggressor.²¹² Self-defense must comply with two principles of CIL—necessity and proportionality.²¹³ Necessity means that self-defense is actually required under the circumstances because a reasonable settlement could not be attained through peaceful means.²¹⁴ Therefore, a state that is subject to an all-out invasion will no doubt be required to use force to overcome the aggressor, whereas a state that is subject to an isolated border skirmish might not need to use force to protect itself.²¹⁵ Proportionality requires self-defense actions to be limited to the amount of force necessary to defeat an ongoing attack or to deter future

²⁰⁹ See WINGFIELD, *supra* note 48, at 46–47 (noting the different opinions legal scholars have on the interplay between Article 51 and CIL regarding anticipatory self-defense); Murphy, *supra* note 49, at 705 (noting the lack of consensus on the legality of anticipatory self-defense due to competing views on the interplay between the U.N. Charter and CIL).

²¹⁰ See Jensen, *supra* note 5, at 219–20; Barkham, *supra* note 29, at 74; Murphy, *supra* note 49, at 706–11 (discussing the strict-constructionist school of thought on the U.N. Charter and armed attacks, which holds that Article 51 of the U.N. Charter consumes all previous CIL relating to self-defense).

²¹¹ See Jensen, *supra* note 5, at 221–26; Barkham, *supra* note 29, at 74–75; Murphy, *supra* note 49, at 706–11 (discussing the imminent threat and qualitative threat schools of thought on CIL and armed attacks, which hold that the right of self-defense under CIL still exists independent of Article 51 of the U.N. Charter).

²¹² See DINSTEIN, *supra* note 184, at 235–37.

²¹³ WINGFIELD, *supra* note 48, at 41–44. *But see* DINSTEIN, *supra* note 184, at 237, 242–43 (noting that self-defense must comply with three principles of CIL—necessity, proportionality and immediacy; under this analysis, immediacy means that self-defense measures cannot be delayed indefinitely and must be taken in a reasonable amount of time after an armed attack). The principle of immediacy originated in relation to anticipatory self-defense, and, for the most part, is accepted as a third principle which only applies to anticipatory self-defense. *See infra* Part IV.D.

²¹⁴ DINSTEIN, *supra* note 184, at 237.

²¹⁵ *Id.*

aggression.²¹⁶ This principle does not require the size and scope of defensive actions to be similar to those of the attack. A defensive action may need to employ significantly greater force than the attacker used to successfully repel the attacker.²¹⁷ The key is to determine the amount of force needed to either defeat the current attack or to deter future attacks. For instance, after an all-out invasion a proportionate response might entail a full-scale war to defeat the aggressor's military, including the use of nuclear weapons.²¹⁸ On the other hand, a proportionate response to an isolated missile strike might be to strike the launching facility for that missile.²¹⁹ These principles define the scope of self-defense responses and explain the reasons behind self-defense requirements.

D. Anticipatory Self-Defense

Anticipatory self-defense is a subset of self-defense.²²⁰ Its basis is that "aggression often begins without shots being fired or borders being crossed."²²¹ Sometimes states will obtain information that reveals that an armed attack is about to be launched against them. Although the attack has not yet occurred, "States can rightfully defend themselves against such violence."²²²

The crux of the issue, therefore, is not who fired the first shot but who embarked upon an apparently irreversible course of action, thereby crossing the legal Rubicon. The casting of the die, rather than the actual opening of fire, is what starts the armed attack. It would be absurd to require that the defending State should sustain and absorb a devastating (perhaps a fatal) blow,

²¹⁶ See Schmitt, *supra* note 57, at 532.

²¹⁷ See *id.*

²¹⁸ See DINSTEIN, *supra* note 184, at 237–42.

²¹⁹ See WINGFIELD, *supra* note 48, at 48.

²²⁰ MICHAEL WALZER, *JUST AND UNJUST WARS* 74 (1977); see also Murphy, *supra* note 49, at 706–11 (noting students of the imminent threat and qualitative threat schools of thought on CIL treat imminent armed attacks as armed attacks for purposes of self-defense). *But see* Murphy, *supra* note 49, at 706–11 (noting some legal scholars strictly construe the U.N. Charter to authorize self-defense only in response to actual armed attacks).

²²¹ *Id.*

²²² *Id.*

only to prove the immaculate conception of self-defence [sic].²²³

Anticipatory self-defense is a long-standing tenet of CIL, dating back to the 1836 *Caroline* case.²²⁴ In *Caroline*, the United Kingdom and the United States agreed that self-defense was lawful in advance of an armed attack, when “the necessity of that self-defense is instant, overwhelming and leaving no choice of means, and no moment for deliberation.”²²⁵ As discussed in Part IV, Section C, anticipatory self-defense is not a universally accepted principle among legal scholars;²²⁶ however, despite ongoing debate, stronger arguments exist in support of anticipatory self-defense as a fundamental axiom of international law.²²⁷ The real question is, when can states act in anticipatory self-defense?

²²³ DINSTEIN, *supra* note 184, at 191. Dinstein calls this interceptive self-defense, arguing that armed attacks should be more broadly construed than invasive force across national borders; however, his justification for interceptive self-defense is the same justification for anticipatory self-defense. The only real distinction between the Dinstein and other legal scholars is the timing of anticipatory self-defense, which shall be addressed in this section. Barkham, *supra* note 29, at 76–77.

²²⁴ See Barkham, *supra* note 29, at 75; Murphy, *supra* note 49, at 705.

²²⁵ WINGFIELD, *supra* note 48, at 47 (quoting THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 675 (Bruno Simma ed. 1994) (quoting then Secretary of State Daniel Webster)).

²²⁶ See *supra* Part IV.C.

²²⁷ Since anticipatory self-defense was a long-standing tenet of international law prior to the U.N. Charter, it is important to note that the English language version of the U.N. Charter states that it does nothing to impair states’ inherent right of self-defense. Furthermore and even more persuasively, the French language version of the Charter, which is equally as authoritative as the English version, preserves the inherent right of nations to act in self-defense in situations where *the member-state is the object of an armed aggression*. Since “armed aggression” is less restrictive than “armed attack,” the choice to use “armed aggression” in the French version supports the view that the drafters intended to preserve the right of self-defense as it existed prior to the Charter. See Murphy, *supra* note 49, at 706–15.

Since the ratification of the U.N. Charter, states have continued to rely on anticipatory self-defense as a justification for war, showing that international custom also supports the continuing right of states to act in anticipatory self-defense. See Murphy, *supra* note 49, at 713; Thomas Franck, *When, If Ever, May States Deploy Military Force Without Prior Security Council Authorization?*, 5 WASH. U. J.L. & POL’Y 51, 59 (2001).

Further supporting anticipatory self-defense as a maxim of international law, the ICJ has found that self-defense was not subsumed by the U.N. Charter. See *Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.)*, 1986 I.C.J. 14, 110 (June 27); see also DINSTEIN, *supra* note 184, at 181 (citing the ICJ’s opinion in *Nicaragua*); Jensen, *supra* note 5, at 221 (citing the ICJ’s opinion in *Nicaragua*).

Finally, respected legal scholars also believe that anticipatory self-defense continues to be a maxim of international law. See WALZER, *supra* note 220, at 82–85; DINSTEIN, *supra* note 184, at 191 (rejecting the doctrine of anticipatory self-defense, but recognizing

The legality of anticipatory self-defense actions depends on the imminency of an attack.²²⁸ Imminency, sometimes called immediacy and sometimes referred to as the third principle of self-defense, supplements the traditional self-defense principles of necessity and proportionality of anticipatory self-defense.²²⁹ Generally speaking, imminency allows a state to use force against an identified aggressor, in advance of an armed attack, to repel the attack before it is launched.²³⁰ Initially, the concept of imminency restricted anticipatory self-defense to situations immediately before an attack, where an attack was detected, but there was no time to deliberate about other means of preventing the attack short of forceful self-defense.²³¹ The principle effectively balanced the victim-state's right to ward off violence against its international obligation to find peaceful means to resolve disputes.²³² However, due to changes in the nature of warfare, imminency has evolved significantly.²³³

Today, imminency allows states to legally employ force in advance of an attack, at the point when (1) evidence shows that an aggressor has committed itself to an armed attack and (2) delaying a response hinders the defender's ability to mount a meaningful defense.²³⁴ Thus, imminency is actually a relative concept,²³⁵ which operates as follows:

Weak States may lawfully act sooner than strong ones in the face of identical threats because they are at greater risk as time passes. In the same vein, it may be necessary to conduct defensive operations against a terrorist group long before a planned attack because there is unlikely to be another opportunity to target terrorists before they strike. . . . In other words, each

the right of interceptive self-defense before an attack occurs); WINGFIELD, *supra* note 48, at 47, 94; Schmitt, *supra* note 57, at 528–36.

²²⁸ See Schmitt, *supra* note 57, at 528–36.

²²⁹ See *id.* at 533.

²³⁰ See *id.* at 533–34.

²³¹ See *id.* (recalling the standards set forth in the *Caroline* case).

²³² See *id.* at 534.

²³³ See *id.* (noting that it has become accepted to invoke anticipatory self-defense earlier and earlier, in advance of an attack, as the consequences of a single attack become more severe (in the case of chemical, biological or nuclear weapons) and as intelligence gathering tools become more advanced (satellite imagery, intercepted electronic communications and other state-of-the-art surveillance techniques)).

²³⁴ See *id.* at 534–35.

²³⁵ See *id.* at 534.

situation presents a case-specific window of opportunity within which a State can foil an impending attack.²³⁶

Finally, just because a single attack may be complete does not mean that future attacks are not imminent. When evidence suggests that an attack is part of an ongoing campaign against a state, such as the terrorist attacks against the United States on 9/11, future armed attacks will be considered imminent and anticipatory self-defense will be authorized.²³⁷ Some scholars support the same conclusion but disagree with the legal rationale behind it, claiming that a proportional response in self-defense to a single armed attack can be far-reaching to deter future attacks, and that anticipatory self-defense is the wrong lens through which to view the response to an ongoing campaign.²³⁸

E. Proportionate Countermeasures/Reprisals

Proportionate countermeasures, also known as reprisals, provide another way for states to address illegal uses of force against them.²³⁹ As discussed in Part IV, Section C, no consensus exists as to what constitutes an armed attack, meaning that a cyberattack could be seen as a use of force below the armed attack threshold.²⁴⁰ As a result, it is important to explore the rights that states have to react to illegal uses of force against them which fall short of an armed attack.

Proportionate countermeasures are an exception to the general rule that states are required to solve their disputes peacefully.²⁴¹ “A reprisal ‘is an act which is unlawful *per se*, unless it can be justified as a countermeasure triggered by an unlawful act and is designed to induce the offending state to return to full compliance with the law.’”²⁴² Should a state decide to use proportionate countermeasures, it must comply with

²³⁶ *Id.*

²³⁷ *See id.* at 535–36.

²³⁸ *See* Murphy, *supra* note 49, at 734–36 (arguing that self-defense allowed the United States to conduct a far reaching campaign against al Qaeda in response to the 9/11 attacks on the grounds of self-defense, not anticipatory self-defense).

²³⁹ *See* WINGFIELD, *supra* note 48, at 85; Jensen, *supra* note 5, at 220.

²⁴⁰ *See supra* Part IV.C.

²⁴¹ *See* WINGFIELD, *supra* note 48, at 84–85.

²⁴² *See id.* at 85 (quoting THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 101 (Bruno Simma ed. 1994)).

the three criteria enumerated by the International Court of Justice (ICJ) in *Gabcikovo-Nagymaros Project*.²⁴³ These criteria are:

In the first place [countermeasures] must be taken in response to a previous international wrongful act of another State and must be directed against that State. . . . Secondly, the injured State must have called upon the State committing the wrongful act to discontinue its wrongful conduct or to make reparation for it. . . . [Third] the effects of a countermeasure must be commensurate with the injury suffered, taking account of the rights in question.²⁴⁴

Reprisals may be carried out in various ways. Economic and political coercion are the two main forms of reprisals; however, reprisals could also include the use of limited cyberattacks against an aggressor.²⁴⁵ Reprisals may not involve the use of force contrary to Article 2(4) of the U.N. Charter;²⁴⁶ however, the consensus among international scholars is that this prohibition really only amounts to a prohibition against armed force.²⁴⁷ While this article contends that states should treat certain cyberattacks as armed attacks, and deal with them using self-defense and anticipatory self-defense legal principles, reprisals provide an important alternate theory for dealing with cyberattacks to those who contend that cyberattacks fall short of the armed attack threshold.²⁴⁸

The general framework of *jus ad bellum* discussed so far has primarily evolved in response to state-on-state attacks. When attacks are carried out by non-state actors across state borders, it complicates the framework governing state responses to the attacks. Since most cyberattacks are carried out by non-state actors, this article will explore *jus ad bellum* in greater depth and explain the intricacies of state responses to attacks by non-state actors.

²⁴³ *Gabcikovo-Nagymaros Project* (Hung. v. Slov.), 1997 I.C.J. 7, 55–56 (Sept. 25) (Merits).

²⁴⁴ *Id.*

²⁴⁵ See WINGFIELD, *supra* note 48, at 84–92.

²⁴⁶ See *id.* at 85.

²⁴⁷ See *id.* at 87 (quoting THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 112 (Bruno Simma ed. 1994)).

²⁴⁸ See *infra* Part VI.A (discussing cyberattacks as armed attacks).

V. Non-State Actors and *Jus ad Bellum*

International cyberattacks by non-state actors complicate the general framework of *jus ad bellum*. Since the prevailing view of international law requires states to attribute an attack to a state or its agents before responding with force,²⁴⁹ states feel obligated to undertake lengthy, time-consuming investigations before responding to cyberattacks, thereby increasing the risks that the cyberattack poses.²⁵⁰ This creates a dilemma for states. While states can trace an attack back to a server in another state, identifying who is at the other end of the electronic connection directing the attack takes more time than states have to decide how to respond to the attack. Thus, the prevailing view of the law forces states into a response crisis during an international cyberattack.²⁵¹

Unfortunately, a lack of state cooperation has exacerbated the response crisis.²⁵² In an ideal world, states would not commit cyberattacks and would assist victim-states in tracking down attackers. Under this utopian paradigm, states could contentedly rely on passive defenses, knowing that attackers who breached their defenses would be hunted down and punished. Unfortunately, this is not the reality, and states are left in limbo during an attack. Yet even if a cyberattack were attributable to a non-state actor, and states wanted to respond with force, they are bound not to intervene in the domestic affairs of other states.²⁵³ Not surprisingly, despite a lack of state cooperation, states attempt to respond via criminal laws, rather than risk unlawfully violating the sovereignty of another state.²⁵⁴

There is, however, a way to avoid the attribution problem and response crisis. When a victim-state can lawfully impute a cyberattack to its state of origin, it can immediately respond with force under the law of war, regardless of whether the attack was conducted by the state itself or by non-state actors within it.²⁵⁵ Thus, imputing state responsibility creates a legal path for states to respond to cyberattacks with active defenses in a timely and effective manner. Given the technological and

²⁴⁹ See Condrón, *supra* note 24, at 415; DINSTEIN, *supra* note 184, at 111.

²⁵⁰ See Condrón, *supra* note 24, at 407–08.

²⁵¹ See *supra* Part II.A (discussing the response crisis).

²⁵² See *id.* (discussing the lack of state cooperation in tracking down attackers).

²⁵³ Hollis, *supra* note 22, at 1049–50. To do so would be a violation of the sovereignty of the other state, and would be in violation of CIL. *Id.*

²⁵⁴ See *supra* Part II.A.

²⁵⁵ See *infra* Part VI.B–C.

diplomatic limitations to timely attack attribution,²⁵⁶ it is crucial for legal scholars to reexamine the legal regime governing state responses to cyberattacks committed by non-state actors through the lens of imputed responsibility.

The legal analysis for determining whether cyberattacks can be imputed to their state of origin starts with the underlying law behind armed attacks by non-state actors. From there, the analysis continues with the duties states have to one another concerning non-state actors within their territory, then moves on to the ways to impute state responsibility for acts by non-state actors, and ends with the legality of certain cross-border operations against other states.

A. Armed Attacks by Non-State Actors

Non-state actors can and have committed armed attacks against states.²⁵⁷ Most legal scholars believe these attacks fall under the law of war.²⁵⁸ This opinion enjoys broad support from all four sources of international law: international conventions, international custom (as evidence of a general principle accepted as law), the general principles of law recognized by civilized nations, and the judicial decisions and teachings of the most highly qualified international legal scholars (as a means for determining the rules of law).²⁵⁹ However, since this opinion is not universally held,²⁶⁰ it is worth discussing at some length.

Of the four sources of international law, international treaties lend the least support for the proposition that non-state actors may commit an armed attack. Their support is, at best, indirect, based on their silence on

²⁵⁶ See *supra* Part II.A (discussing the attribution problem).

²⁵⁷ See DINSTEIN, *supra* note 184, at 187, 204; WALZER, *supra* note 220, at 197–206 (discussing various terrorist campaigns); Schmitt, *supra* note 57, at 536–40 (discussing the Sept. 11, 2001 terrorist attacks by al Qaeda).

²⁵⁸ See DINSTEIN, *supra* note 184, at 204–08; Michael Schmitt, *Counter-Terrorism and the Use of Force in International Law*, in INTERNATIONAL LAW AND THE WAR ON TERROR 7, 33–47 (Fred L. Borch & Paul S. Wilson eds., Naval War College 2003); Schmitt, *supra* note 57, at 536–40; Rein Mullerson, *Jus Ad Bellum and International Terrorism*, in INTERNATIONAL LAW AND THE WAR ON TERROR 75, 106–11 (Fred L. Borch & Paul S. Wilson eds., Naval War College 2003).

²⁵⁹ See WINGFIELD, *supra* note 48, at 72 (quoting Statute of the International Court of Justice art. 38(1), June 26, 1945, 59 Stat. 1055, 1060 (1945)).

²⁶⁰ Some scholars argue that the law of war only governs attacks by states. Schmitt, *supra* note 57, at 536.

the subject. This silence allows states to infer support because no treaty has ever prohibited states from treating attacks by non-state actors as acts of war, despite the opportunity to do so. As noted earlier, modern *jus ad bellum* analysis starts with the U.N. Charter.²⁶¹ However, the Charter was written to govern armed conflict between states.²⁶² As a result, the Charter is silent about armed attacks by non-state actors.²⁶³ While it appears that the minimalist language of Article 51 allows a state to respond in self-defense to armed attacks against it,²⁶⁴ the lack of any specific language on point forces us to look to the other three sources of international law to determine the controlling standards for armed attacks by non-state actors.

Although the issue of non-state actors was not originally envisioned in the drafting of the U.N. Charter, analysis of CIL reveals that “[i]t is incontrovertible that states now treat the law of self-defense as applicable to acts by non-state actors.”²⁶⁵ The international community’s response to the terrorist attacks of September 11, 2001 (9/11) crystallized the validity of this principle.²⁶⁶ Following the 9/11 attacks, the U.N. Security Council passed Resolution 1368, characterizing the attacks as a threat to international peace and security under Article 39 of the Charter and reaffirming the United States’ inherent right to engage in either individual or collective self-defense in accordance with Article 51 of the

²⁶¹ See *supra* Part IV, intro.

²⁶² See U.N. Charter art. 1 (stating that its purpose is to maintain international peace and security through the regulation of state action); Schmitt, *supra* note 57, at 536 (noting that the U.N. Charter was drafted to regulate state-on-state armed conflicts); Mullerson, *supra* note 258, at 112 (stating that there is little doubt that the drafters of the Charter had not contemplated armed attacks by non-state actors).

²⁶³ See generally U.N. Charter (making no mention of non-state actors anywhere in the Charter).

²⁶⁴ *Id.* art. 51; DINSTEIN, *supra* note 184, at 204 (noting that Article 51 regulates state responses to armed attacks, but never specifies the character of the perpetrator of the attacks, therefore implying that self-defense could be invoked against states or non-state actors); Schmitt, *supra* note 258, at 33–34 (noting that Chapter VII of the Charter, which includes both Articles 39 and 51, dictates what states may do in the face of threats to international peace and security and acts of aggression, without ever stating what those might be). *But see* Schmitt, *supra* note 57, at 536 (noting a number of commentators assert that because the U.N. Charter does not specifically address armed attacks by non-state actors, those attacks therefore fall outside the scope of the law of war and should, instead, be governed by international and domestic criminal laws).

²⁶⁵ Schmitt, *supra* note 57, at 539.

²⁶⁶ See DINSTEIN, *supra* note 184, at 207–08; Schmitt, *supra* note 258, at 7–47; Schmitt, *supra* note 57, at 536–40; Mullerson, *supra* note 258, at 84, 106–19.

Charter.²⁶⁷ Two weeks after the attacks, when it appeared clear that al Qaeda was behind the attacks, the Security Council passed Resolution 1373, once again affirming the United States' inherent right of self-defense in response to the attacks.²⁶⁸ These Security Council declarations are particularly significant because the 9/11 attacks could have been dealt with under Article 42 of the Charter, but instead were dealt with under Article 51, even though the attacks were committed by non-state actors.²⁶⁹ The North Atlantic Treaty Organization, the Organization of American States, and Australia all made similar declarations, invoking the collective self-defense provisions of their mutual defense treaties, to assist the United States in its response to the 9/11 attacks.²⁷⁰ The statements and actions of scores of other states, including major states such as Russia, China, India, Japan, South Korea, Pakistan, Saudi Arabia, and Egypt, lend support to the principle that attacks by non-state actors fall under the law of war.²⁷¹ Finally, this principle was supported by the ICJ in its 2004 Advisory Opinion in *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*,²⁷² as well as from the publications of legal scholars.²⁷³

²⁶⁷ See Schmitt, *supra* note 57, at 536–37 (noting that at the time Resolution 1368 was passed, no one believed that a state was behind the attacks, yet the attacks were found to be a threat to international peace and security under Article 39).

²⁶⁸ See *id.* at 537.

²⁶⁹ See Schmitt, *supra* note 258, at 16. Had the Security Council wanted to deal with the 9/11 attacks under Article 42 of the U.N. Charter, it could have authorized the United States, a coalition of forces, or a regional organization to use force pursuant to it, “as the Council is entitled to do in the face of a ‘threat to the peace, breach of peace or act of aggression.’” *Id.* (quoting Article 42 of the U.N. Charter).

²⁷⁰ The NATO unanimously invoked Article 5 of the Washington Treaty, based on Article 51 of the U.N. Charter, which provides for collective self-defense in response to armed attacks against a member-state. The Organization of American States invoked the collective self-defense provision of the Rio Treaty. Australia invoked Article IV of the ANZUS Treaty. See *id.* at 16–18.

²⁷¹ See Schmitt, *supra* note 258, at 18; Schmitt, *supra* note 57, at 538–39.

²⁷² See DINSTEIN, *supra* note 184, at 204 (referencing the Separate Opinions of Judge Higgins and Judge Kooijmans, as well as the Declaration of Judge Buergenthal, in *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, 2004, 43 I.L.M. 1009, 1063, 1072, 1079 (2004)). While the ICJ held that Israel could not respond in self-defense to terrorist attacks from non-state actors in this case, the court explicitly stated this was because Israel never asserted the acts were imputable to a state. *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, 2004, 43 I.L.M. 1009, 1050 (2004). Thus, the case shows that attacks by non-state actors fall under the law of war, but that the law of war only permits states to respond in self-defense when the actions of the non-state actors are imputable to a state, which was not the case here.

²⁷³ See DINSTEIN, *supra* note 184, at 204–08; Schmitt, *supra* note 258, at 33–47; Schmitt, *supra* note 57, at 536–40; Mullerson, *supra* note 258, at 106–11.

While attacks by non-state actors fall under the law of war, the law of war only allows states to forcibly respond to these attacks when the attacks are imputable to a state,²⁷⁴ meaning the state also bears some responsibility for the actions of the non-state actors. The next step of the analysis toward imputing state responsibility for these attacks is, therefore, to examine the duties that states have concerning non-state actors within their territory.

B. Duties Between States

“It is a long established principle of international law that ‘a state is bound to use due diligence to prevent the commission within its dominions of criminal acts against another nation or its people.’”²⁷⁵ This principle is reflected in numerous state declarations, judicial opinions, and publications from leading scholars.²⁷⁶ State declarations that support this principle include the following: the 1970 Declaration on Friendly Relations, which urges states to “refrain from . . . acquiescing [to] organized activities within [their] territory directed towards the commission of [civil strife or terrorism in another State];”²⁷⁷ the 1994 Declaration on Measures to Eliminate Terrorism;²⁷⁸ and the 1996 Declaration on the Strengthening of International Security, which stated that states “must refrain from organizing, instigating, assisting or participating in terrorist acts in territories of other states, or from acquiescing in or encouraging activities within their territories directed towards the commission of such acts.”²⁷⁹ International case law also

²⁷⁴ See *supra* note 272 and accompanying text; *infra* Part V.C–D.

²⁷⁵ Schmitt, *supra* note 57, at 540–41 (quoting John Bassett Moore in *S.S. Lotus* (Fr. v. Turk.) 1927 P.C.I.J. (ser. A) No. 10, at 4, 88 (Moore, J., dissenting)).

²⁷⁶ See DINSTEIN, *supra* note 184, at 205–06; Schmitt, *supra* note 258, at 39–40, 48; Schmitt, *supra* note 57, at 541.

²⁷⁷ Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among states in Accordance with the Charter of the United Nations, G.A. Res. 2625, ¶ 1, U.N. GAOR, 25th Sess., Annex, Agenda Item 85, U.N. Doc. A/Res/2625 (Oct. 24, 1970); see also Vincent-Joel Proulx, *Babysitting Terrorists: Should States Be Strictly Liable for Failing to Prevent Transborder Attacks?*, 23 BERKELEY J. INT’L L. 615, 629 (2005); Schmitt, *supra* note 258, at 39–40 (quoting the 1970 Declaration on Friendly Relations).

²⁷⁸ Schmitt, *supra* note 258, at 40 (citing the 1994 Declaration on Measures to Eliminate International Terrorism, G.A. Res. 49/60, U.N. GAOR 6th Comm., 49th Sess., 84th plen. mtg., Annex, U.N. Doc. A/49/743 (1994)).

²⁷⁹ *Id.* at 48 (quoting Declaration to Supplement the 1994 Declaration on Measures to Eliminate International Terrorism, G.A. Res. 51/210, U.N. GAOR 6th Comm., 51st Sess., 88th plen. mtg., Annex, U.N. Doc. A/51/631 (1996)).

supports this principle. In *Corfu Channel*, “the International Court of Justice pronounced that every state is under an obligation ‘not to allow knowingly its territory to be used for acts contrary to the rights of other States.’”²⁸⁰ In *Tehran*, the ICJ re-affirmed that States “are required under international law to take appropriate acts in order to protect the interests” of other states from non-state actors within their borders.²⁸¹ Finally, scholars have noted this principle “is so widely recognized that it should not fuel a debate.”²⁸²

In short, it is clear from state practice and *opinio juris* that states have an affirmative duty to prevent non-state actors within their borders from committing armed attacks on other states.²⁸³ Toleration of such attacks constitutes a crime under international law.²⁸⁴ Thus, “a host-State that has the capability to prevent [an armed attack by non-state actors] but fails to do so will inherently fail to fulfill its duty” under international law.²⁸⁵ However, it is not realistic to expect states to completely prevent armed attacks by non-state actors from ever occurring.²⁸⁶ As a result, the dispositive factor in evaluating whether states live up to their duty “will lie, rather, in the conduct of the host-state itself in addressing the potential threat and in attaining a realistic result in light of the factual circumstances.”²⁸⁷

²⁸⁰ DINSTEIN, *supra* note 184, at 205–06 (quoting *Corfu Channel* case (Merits), 1949 I.C.J. Rep. 4, 22 (Apr. 9)); *see also* Schmitt, *supra* note 258, at 49.

²⁸¹ DINSTEIN, *supra* note 184, at 206 (citing Case Concerning United States Diplomatic and Consular Staff in Tehran, 1980 I.C.J. Rep. 3, 32–33, 44 (May 24)).

²⁸² Proulx, *supra* note 277, at 629–60; *see also* DINSTEIN, *supra* note 184, at 205–06 (noting further support from Ian Brownlie); Proulx, *supra* note 277, at 659–66 (noting further support from Davis Brown, Lee Feinstein, Matthew Lippman and Anne-Marie Slaughter); Schmitt, *supra* note 258, at 39–40, 48; Schmitt, *supra* note 57, at 540–41.

²⁸³ *See* Proulx, *supra* note 277, at 660 (referencing this duty in regard to terrorism). State practice and *opinio juris* are the two elements that the international legal community recognizes as the basis for CIL. Jeremy Marsh, *Lex Lata or Lex Ferenda? Rule 45 of the ICRC Study on Customary International Humanitarian Law*, 198 MIL. L. REV. 116, 121 (2008). State practices, state declarations, and U.N. General Assembly declarations and resolutions are all forms of state practice. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 102 (1987) [hereinafter RESTATEMENT]. Furthermore, these declarations and resolutions serve as evidence of *opinio juris*. *Id.* § 103.

²⁸⁴ *See* DINSTEIN, *supra* note 184, at 207.

²⁸⁵ Proulx, *supra* note 277, at 660 (discussing host-states’ duty to stop acts of terrorism against other states when those attacks originate from within their borders).

²⁸⁶ *See id.* at 662.

²⁸⁷ *Id.*

In and of itself, the duty to prevent attacks does not make states responsible for every cross-border attack by non-state actors that emanates from their territory. However, it does bridge the gap between the actions of non-state actors and state responsibility for those acts. The next section completes the analysis of imputing state responsibility for the cross-border attacks of non-state actors.

C. Imputing State Responsibility for Acts by Non-State Actors

The question of a state's legal responsibility for the acts of non-state actors has evolved significantly during the past thirty-seven years.²⁸⁸ Before 1972, states were generally not viewed as legally responsible for the acts of private or non-state actors.²⁸⁹ Only the actions of the host-state's organs were imputable to it, and state responsibility arose only from acts by qualifying "agents" of the state.²⁹⁰ Qualified agents amounted to actors over whom a state exercised direct authority, and whom the state directed to conduct the acts.²⁹¹ As time passed, international law shifted away from a direct control approach and moved toward an indirect responsibility approach regarding the acts of non-state actors.²⁹² This shift began with the International Tribunal for the former Yugoslavia's (ICTY) seminal opinion on state responsibility, in which it revised the effective control test to impute host-state responsibility for the actions of groups of non-state actors over whom a state had "overall control."²⁹³ While overall control is still a form of direct control, the

²⁸⁸ See *id.* at 616–19.

²⁸⁹ See *id.* at 619.

²⁹⁰ See *id.* at 619–20.

²⁹¹ See *id.* at 620–21. The standard for assessing state responsibility under this paradigm was the "effective control test," which was first espoused by the ICJ in *Nicaragua*. In *Nicaragua*, the United States financed, organized, trained, supplied, and equipped contra rebels who were fighting against the government of Nicaragua. Yet despite the contras' dependence on the United States, the ICJ refused to hold the United States legally liable for the contras' actions. The court took the view that while the United States provided decisive support to the contras, a state was not legally responsible for the actions of non-state actors unless the state "had effective control of the military or paramilitary operations in the course of which the alleged violations were committed." *Id.* at 620–21 (quoting the *Nicaragua* case). But see Mark Baker, *Terrorism and the Inherent Right of Self-Defense*, 10 HOUS. J. INT'L L. 25, 41 (1987) (raising the question that state responsibility might arise from the mere toleration of terrorist groups within a host-state's borders, without providing any active support).

²⁹² See Proulx, *supra* note 277, at 621–23.

²⁹³ See *id.* (referring to the *Tadic* case, Prosecutor v. Tadic, Case No. IT-94-1-A, I.C.T.Y. App. Ch., at 49 (July 15, 1999), in which the court held that states were responsible for

opinion marked a significant relaxation of the standard for state responsibility.²⁹⁴ The shift to indirect responsibility continued through the middle of 2001, with a general consensus emerging that any breach of a host-state's international obligations to other nations, whether from treaty law or customary law, resulted in international responsibility for the host-state.²⁹⁵ These breaches can result from a state's acts or its failure to act.²⁹⁶ This consensus solidified following the 9/11 terrorist

the acts of militarized groups when the state coordinated or helped in the general planning of the group's military activity). This shift was not without precedent. In 1923, several members of an international commission, who were overseeing the delimitation of the Greek-Albanian border, were assassinated in Greek territory. The League of Nations organized a special committee to address the legal questions involved. While the committee found that the evidence did not support Greek responsibility, "it opined that a host-state could be held responsible in like circumstances if it 'neglected to take all reasonable measures for the prevention of the crime and pursuit, arrest and bringing to justice of the criminal.'" *Id.* at 627 (quoting the *Tellini* case, 4 League of Nations O.J. 524 (1924)).

While not yet culminating in a shift in international law, further precedent for the shift to indirect state responsibility comes from the *Tehran* case. In 1979, Iranian student militants took over the U.S. embassy and consulates in Iran. The ICJ found no evidence that the militants were operating on the direct behest of the Iranian State, and therefore found that the attacks could not be attributed to the State. However, the court laid some blame on Iran, finding that Iran had not lived up to its international obligation to protect the victims of the attack. It justified this position on the grounds that Iran bore indirect responsibility for its failure "to take any 'appropriate steps' . . . either to prevent this attack or to stop it before it reached its completion.'" *Id.* at 628 (quoting from the *Tehran* case, *Tehran Hostages Case (U.S. v. Iran)*, 1980 I.C.J. 64 (May 24)).

Lastly, the trend towards indirect responsibility was evident in several cases before the Security Council in the 1990s. In these cases concerning international terrorism, the Security Council recognized the rights of injured states to pursue terrorists into other states to eliminate their bases of operation. Examples of such were in 1995 and 1996 when Turkey pursued Kurdish irregulars on Iraqi soil; in 1992 and 1995 when Senegal entered Guinea-Bissau to strike at safe havens used by opposition forces; and in 1998 when the United States bombed parts of Afghanistan following terrorist attacks on U.S. embassies in Tanzania and Kenya. *See id.* at 630–31.

²⁹⁴ *See id.* at 621.

²⁹⁵ *See id.* at 622–23 (referencing the International Law Commission's adoption of the 2001 Draft Articles on the Responsibility of States for Internationally Wrongful Acts, U.N. Doc. A/CN.4/L.602/Rev. 1 (2001)). After the International Law Commission approved the Draft Articles, the U.N. General Assembly took note of them and commended them to state governments on two different occasions; first in 2001 and next in 2004. *See* G.A. Res. 56/83, U.N. Doc. A/RES/56/83 (Jan. 28, 2002); G.A. Res. 59/35, U.N. Doc. A/RES/59/35 (Dec. 16, 2004).

²⁹⁶ *See* Proulx, *supra* note 277, at 626 (referencing Article 2 of the 2001 Draft Articles of the Responsibility of States for Internationally Wrongful Acts).

attacks on the United States, bringing us to today's framework for state responsibility.²⁹⁷

September 11, 2001 marked the culmination of the shift of state responsibility from the paradigm of direct control to indirect responsibility.²⁹⁸ On that date, al Qaeda terrorists hijacked four airplanes, flew three of them into buildings in the United States, and killed more than three thousand U.S. citizens in what was widely recognized as an armed attack.²⁹⁹ Al Qaeda was based in Afghanistan, which at the time was ruled by the Taliban.³⁰⁰ While the Taliban harbored al Qaeda and occasionally provided it limited logistical support, the Taliban did not exercise effective or even overall control over al Qaeda.³⁰¹ Further distancing the Taliban from 9/11 is the lack of evidence suggesting that the Taliban knew of the 9/11 attacks beforehand, or even endorsed them after the fact.³⁰² Yet despite all of this, it was internationally accepted that al Qaeda's acts were legally imputable to the Taliban, and thus to Afghanistan, because it had harbored and sheltered al Qaeda, and refused to stop doing so, even after being warned to stop.³⁰³

Thus, following 9/11, state responsibility may be implied based on a state's failure to fulfill its international duty to prevent non-state actors from using its territory to attack other states.³⁰⁴ The contemporary doctrine of state responsibility does not require a causal link between a wrongdoer and a host-state; rather, it focuses on the state's duty to prevent attacks from its territory into that of another.³⁰⁵ "Hence, a state's passiveness or indifference toward [a non-state actor's] agendas within its own territory might trigger its responsibility, possibly on the same scale as though it had actively participated in the planning."³⁰⁶ Much of the legal analysis of whether a state is responsible will "turn[] on an *ex-*

²⁹⁷ See generally *id.* at 618–19, 625–43 (explaining the shift from direct responsibility to indirect responsibility for the acts of non-state actors and the state of the law post-9/11).

²⁹⁸ See *id.* at 634–52.

²⁹⁹ Schmitt, *supra* note 258, at 33.

³⁰⁰ See Proulx, *supra* note 277, at 634–37.

³⁰¹ See *id.* at 635–36.

³⁰² See *id.* at 636.

³⁰³ See *id.* at 637–41.

³⁰⁴ See TAL BECKER, TERRORISM AND THE STATE: RETHINKING THE RULES OF STATE RESPONSIBILITY 3 (2006); 2001 Draft Articles on the Responsibility of States for Internationally Wrongful Acts, U.N. Doc. A/CN.4/L.602/ Rev. 1 (2001).

³⁰⁵ See BECKER, *supra* note 304, at 3; Proulx, *supra* note 277, at 633.

³⁰⁶ Proulx, *supra* note 277, at 624.

post facto analysis of whether the state could have put more effort into preventing the . . . attack.”³⁰⁷

However, even when state responsibility is imputed for the armed attacks of non-state actors, states may still be forbidden from responding with force. The final step in the legal analysis for determining when victim-states can forcibly respond to the armed attacks of non-state actors ends with an examination of the legality of cross-border operations against other states.

D. Cross-Border Operations

Cross-border operations into the territory of an offending state are the natural consequence of imputed state responsibility for the armed attacks of non-state actors.³⁰⁸ However, states must meet a number of legal requirements before they may pursue a non-state aggressor into another state in self-defense. To understand the rationale behind why states may breach a host-state’s general right to territorial integrity in self-defense and the requirements states must meet in order to do so, one must first look to the U.N. Charter’s general prohibition on using force against another state.

The right of territorial integrity generally gives way to the right of self-defense.³⁰⁹ The principle underlying this balancing act is that when one state violates another state’s territorial integrity, it forfeits its own right to territorial integrity. Of course, this principle evolved out of state-on-state attacks. Nonetheless, it may be applied in a similar manner when states are indirectly responsible for the violations of another state’s territorial integrity by non-state actors.

Ascertaining the appropriate balance between one State’s right to territorial integrity and another’s right to self-defense depends in part on the extent to which the former has complied with its own international obligations vis-à-vis the latter. It is a long-established principle of international law that “a State is bound to

³⁰⁷ *Id.* at 663–64.

³⁰⁸ See Schmitt, *supra* note 57, at 540–41.

³⁰⁹ After all, “it is manifestly legal to cross into another State to conduct military operations in self-defense if it is that State which has committed aggression.” *Id.* at 540.

use due diligence to prevent the commission within its dominions of criminal acts against another nation or its people.”

....

If a State is unable or unwilling to comply with this obligation, the victim State may then cross into the offending State to conduct defensive operations.

....

It cannot be otherwise, for the unwillingness or inability of one State to meet its legal obligations cannot deprive other States of the most important right found in international law, the right to defend oneself against an armed attack.³¹⁰

As always, before a state resorts to self-defense, it must ensure that it meets the criteria of necessity, proportionality, and, if using the subset of anticipatory-self defense, imminency.³¹¹ Effectively, a state must have no viable alternatives to the use of force, and it must limit its use of force to securing its defensive objectives.³¹² Naturally, no two situations are alike, and justifications for self-defense are case-specific.

The application of these requirements may vary depending on whether the acts of the non-state actors were imputed based on direct control or indirect attribution. In cases of direct control, the victim-state may immediately impute responsibility to the host-state and act in self-defense against it and the non-state actors inside it.³¹³ In cases of indirect attribution, victim-states must overcome another hurdle before conducting cross-border operations. Namely, the victim-state must ensure that it has properly linked the actions of the non-state actors to the host-state; this may be achieved by issuing a demand to the sanctuary state to “comply with its obligation to prevent its territory from being improperly used.”³¹⁴ The sanctuary state must then act against the non-

³¹⁰ *Id.* at 540–42 (quoting *S.S. Lotus (Fr. v. Turk.)* 1927 P.C.I.J. (ser. A) No. 10, at 4, 88 (Moore, J., dissenting)).

³¹¹ *See id.* at 542.

³¹² *See id.*

³¹³ *See id.* at 543.

³¹⁴ *Id.* at 542.

state actors, or willingly allow the victim-state to enter its territory and mount operations against the non-state actors.³¹⁵ Should the host-state be unwilling to meet these requirements, the victim-state can fully impute responsibility and conduct its cross-border operations into the host-state.³¹⁶ However, in doing so, the victim-state must limit its targets to the non-state actors, unless the host-state uses force to oppose the lawful cross-border operations.³¹⁷

There are numerous examples of internationally accepted cross-border operations into states that were indirectly responsible for the actions of non-state actors. Examples prior to 9/11 include: Turkey's entrance into Iraq in 1995 to pursue Kurdish irregulars; Senegal's entrances into Guinea-Bissau in 1992 and 1995 to strike safe havens used by opposition forces; and the U.S. bombings of Afghanistan in 1998 to strike at terrorist training camps.³¹⁸ Post-9/11 examples include Israel's initial entrance into Lebanon in 2006, following Hezbollah's raid into Israel,³¹⁹ and Turkey's air strikes into Iraq in 2007 against Kurdish irregulars.³²⁰

Based on the foregoing analysis, it is evident that victim-states may forcibly respond to armed attacks by non-state actors located in another state when host-states violate their duty to prevent those attacks. With cyberattacks, imputing state responsibility in this manner provides states a legal path to utilize active defenses without having to conclusively attribute an attack to a state or its agents. In effect, imputing responsibility is the equivalent of attributing the attack to the state or its agents. Thus, imputing responsibility provides states a way around the attribution problem and response crisis. However, just because a legal pathway exists to employ active defenses does not mean that responding to cyberattacks by non-state actors lends itself to this framework. As a result, it is imperative to explain why cyberattacks constitute armed attacks, what a state's duty to prevent cyberattacks means, and the

³¹⁵ See *id.* at 543.

³¹⁶ See Proulx, *supra* note 277, at 641–42; Schmitt, *supra* note 57, at 543; Mullerson, *supra* note 258, at 109.

³¹⁷ See Schmitt, *supra* note 57, at 543.

³¹⁸ See Proulx, *supra* note 277, at 630–31.

³¹⁹ See Greg Myre & Steven Erlanger, *Clashes Spread to Lebanon as Hezbollah Raids Israel*, N.Y. TIMES, July 13, 2006, at A1.

³²⁰ See Sebnem Arsu & Stephen Farrell, *Turkey Bombs Kurds in Iraq; 2 Sides Differ on Casualties*, N.Y. TIMES, Dec. 23, 2007, at A27.

factual circumstances that would allow a victim-state to forcibly respond to a cyberattack.

VI. Analyzing Cyberattacks under *Jus ad Bellum*

Cyberattacks represent a conundrum for legal scholars. Cyberattacks come in many different forms, their destructive potential limited only by the creativity and skill of the attackers behind them.³²¹ While it may seem intuitive that such attacks can constitute armed attacks, especially in light of their ability to injure or kill, the legal community has been reluctant to classify them this way because they do not resemble “classic attack[s] with traditional military force.”³²² Further clouding the legal waters are the erroneous views of states and scholars alike on the need for states to attribute cyberattacks to a state or its agents before responding with force under the law of war. While it is true that cyberattacks do not resemble traditional armed attacks, and that cyberattacks are difficult to attribute, neither of these characteristics of cyberattacks should preclude states from responding with force under the law of war. This part explores different analytical models for assessing armed attacks, the logical meaning of the duty of prevention as it relates to cyberattacks, and the technological capacity of programs to trace attacks back to their point of origin. It concludes with the position that states may legally use active defenses against cyberattacks originating from states that violate their duty to prevent them.

A. Cyberattacks as Armed Attacks

Victim-states must be able to classify a cyberattack as an armed attack or imminent armed attack before responding with active defenses. Armed attacks and imminent armed attacks are the triggers that allow states to respond in self-defense or anticipatory self-defense.³²³ Ideally, clear rules would be in place classifying cyberattacks as armed attacks,

³²¹ WINGFIELD, *supra* note 48, at 100; *see also* Part III.A–B.

³²² THOMAS WINGFIELD, WHEN IS A CYBERATTACK AN “ARMED ATTACK?”: LEGAL THRESHOLDS FOR DISTINGUISHING MILITARY ACTIVITIES IN CYBERSPACE 6 (Cyber Conflict Studies Assoc. 2006); *see also* GREENBERG ET AL., *supra* note 24, at xvii–xviii (noting the ambiguous state of international law regarding cyberattack classification).

³²³ *See supra* Part IV.C–D.

imminent armed attacks, or lesser uses of force.³²⁴ Unfortunately, since cyberattacks are a relatively new attack form, international efforts to classify them are still in their infancy,³²⁵ even though the core legal principles governing armed attacks are well-settled.³²⁶ This has left whether cyberattacks can qualify as armed attacks as open questions in international law.³²⁷ To answer these questions, this section examines the core legal principles governing armed attacks, applies them to cyberattacks, explains why cyberattacks can qualify as armed attacks, and attempts to provide some insight into which cyberattacks should be considered armed attacks.

“Armed attack” is not defined by any international convention.³²⁸ As a result, its meaning has been left open to interpretation by states and scholars. While this might sound problematic, it is not. The framework for analyzing armed attacks is relatively well-settled, as are the core legal principles governing its meaning.³²⁹ The international community generally accepts Jean S. Pictet’s scope, duration, and intensity test as the starting point for evaluating whether a particular use of force constitutes an armed attack.³³⁰ Under Pictet’s test, a use of force is an armed attack

³²⁴ See WINGFIELD, *supra* note 322, at 1–2, 13. State coercion comes in three different forms: threats to international peace and security, uses of force, and armed attacks. *Id.* at 2. Threats to international peace and security and uses of force are both prohibited by Article 2(4) of the U.N. Charter. Armed attacks, including imminent armed attacks, are a more specific subset of uses of force that trigger a victim-state’s inherent right of self-defense in response to them under Article 51 of the U.N. Charter. *See id.* at 4–5.

³²⁵ *Id.* at 2–3, 13.

³²⁶ *Id.* at 12.

³²⁷ *Id.*

³²⁸ See WINGFIELD, *supra* note 48, at 73 (noting the failure of international treaties to define “use of force,” “armed force” or “armed attack”).

³²⁹ See WINGFIELD, *supra* note 322, at 12.

³³⁰ See SHARP, *supra* note 24, at 57–58 (referencing COMMENTARY ON THE GENEVA CONVENTION RELATIVE TO THE PROTECTION OF CIVILIAN PERSONS IN TIME OF WAR 17–21 (Jean S. Pictet ed., 1958)); WINGFIELD, *supra* note 48, at 57, 60–68 (referencing COMMENTARY ON THE GENEVA CONVENTION RELATIVE TO THE PROTECTION OF CIVILIAN PERSONS IN TIME OF WAR 17–21 (Jean S. Pictet ed., 1958)). Courts and scholars have also used a similar “scale and effects” test to judge whether a particular attack rises to the level of an armed attack or constitutes a lesser use of force. *See Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.)*, 1986 I.C.J. 14, 214–16 (June 27); DINSTEIN, *supra* note 184, at 193–96 (using the “scale and effects” test from the *Nicaragua* case to assess armed attacks).

Pictet formulated this test to help clarify when international armed conflict exists under Common Article 2 of the Geneva Conventions. *See SHARP, supra* note 24, at 57–58; WINGFIELD, *supra* note 48, at 57–60. Common Article 2 expresses three circumstances under which international armed conflict exists, and is widely accepted as

when it is of sufficient scope, duration, and intensity.³³¹ Of course, as is the case with many international legal concepts, states, non-governmental organizations, and scholars all interpret the scope, duration, and intensity test differently.³³²

State declarations help flesh out which uses of force are of sufficient scope, duration, and intensity to constitute an armed attack. Harkening back to the French language version of the U.N. Charter, which refers to “armed aggression” rather than an “armed attack,” the U.N. General Assembly passed the Definition of Aggression resolution in 1974.³³³ The resolution requires an attack to be of “sufficient gravity” before it is considered an armed attack.³³⁴ While the resolution never defines armed attacks, it provides examples that are widely accepted by the international community.³³⁵ Unfortunately, the list of armed attacks from

the transition point between peace and war. WINGFIELD, *supra* note 48, at 57. The Common Article 2 circumstances are a declared war between states, the partial or total occupation of another state, or any other armed conflict between states (also known as *de facto* hostilities). Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31 [hereinafter Geneva I]. Once any of these circumstances are met, the threshold between peace and armed conflict is crossed, and the full body of the law of war applies in its entirety. *See* WINGFIELD, *supra* note 48, at 57–60. Since the first two situations are relatively straightforward, the bulk of the law focuses on what constitutes an armed conflict. *See id.*

The term “Geneva Conventions” generally refers to the four Geneva Conventions of 1949. Article 2 of each convention is exactly the same, which is why it is called a common article. Individual citations are as follows: Geneva I, *supra* note 330; Geneva Convention for the Amelioration of the Condition of the Wounded, and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287.

³³¹ *See* WINGFIELD, *supra* note 48, at 57.

³³² *See id.* at 60–68, 111–23 (noting disagreements between the International Committee of the Red Cross’s interpretation and the United States’ interpretation, and reviewing different methods for evaluating the scope, duration, and intensity cyberattacks); Brown, *supra* note 51, at 187–89 (discussing instrument-based evaluations of armed attacks versus effects-based evaluations of armed attacks).

³³³ *See* WINGFIELD, *supra* note 48, at 111 (2000) (referencing Definition of Aggression, G.A. Res. 3314, U.N. GAOR, 29th Sess., U.N. Doc. A/RES/3314 (Dec. 14, 1974)).

³³⁴ Definition of Aggression, G.A. Res. 3314, Annex, art. 2, U.N. GAOR, 29th Sess., U.N. Doc. A/RES/3314/Annex (Dec. 14, 1974) (noting that the uses of force “shall constitute *prima facie* evidence of an act of aggression although the Security Council may . . . conclude that a determination that an act of aggression has been committed would not be justified in the light of other relevant circumstances, including the fact that the acts concerned or their consequences are not of sufficient gravity”).

³³⁵ *See* WINGFIELD, *supra* note 48, at 111. Its view of what constitutes an armed attack

the resolution is not comprehensive, as it only deals with conventional attacks.³³⁶ While the resolution has helped settle the meaning of armed attacks for conventional attacks, the more technology has advanced, the more attacks have come in forms not previously covered by state declarations and practices.³³⁷ Consequently, states recognize that

encompasses the following:

- (a) *Invasion, bombardment and cross-border shooting.* These examples represent the classic cases of armed attacks, provided “that the military actions are on a certain scale and have a major effect, and are thus not to be considered mere frontier incidents.”
- (b) *Blockade.* An effective blocking of a state’s ports or coasts by the armed forces of another state is an armed attack. The barring of passage for land-locked states to the open sea across another state’s territory has not been accepted as an armed attack.
- (c) *Attack on the land, sea or air forces or on the civilian marine and air fleets.* An armed attack occurs when the armed forces of one state attack the land, sea, or air forces, or the civilian marine and air fleets, of another state. The regular forces of a state, wherever they are, always have the right to defend themselves by military force.
- (d) *Breach of stationing agreements.* An armed attack may occur when a state uses its armed forces within the territory of another state in contravention of the conditions provided for in the agreement, or any extension of their presence beyond the termination of the agreement; provided, however, that the breach of the terms of the agreement has the effect of an invasion or occupation.
- (e) *Placing territory at another state’s disposal.* The voluntary action of a state in allowing another state to use its territory for committing an armed attack is also an armed attack.
- (f) *Participation in the use of force by military organized unofficial groups.* It is widely accepted that indirect force falls under the definition of armed attack. The sending of armed bands to use force in another state makes the armed bands a *de facto* state agent, thus the sending state has engaged in an armed attack. Similarly, “substantial involvement” in the activities of an armed band may also constitute an armed attack.

Id. at 111–12 (quoting THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 669–74 (Bruno Simma ed. 1994)).

³³⁶ See *id.* at 112–15 (noting that the use of bacteriological, biological, and chemical agents against another state is considered an armed attack, despite not being listed in the Definition of Aggression resolution).

³³⁷ See WINGFIELD, *supra* note 48, at 113–15; QIAO LIANG & WANG WIANGSUI, UNRESTRICTED WARFARE 1–5 (1999) (speculating that technological advancement and globalization are changing warfare so that future wars will be carried out using non-military war operations, such as cyberattacks, in addition to conventional military force).

unconventional uses of force may warrant treatment as an armed attack when their scope, duration, and intensity are of sufficient gravity.³³⁸ As a result, states are continually making proclamations about new methods of warfare, slowly shaping the paradigm for classifying armed attacks.³³⁹

Scholars have advanced several analytical models to deal with unconventional attacks, such as cyberattacks, to help ease attack classification and put the scope, duration, and intensity analysis into more concrete terms.³⁴⁰ These models are especially relevant to cyberattacks because they straddle the line between criminal activity and armed warfare.³⁴¹ There are three main analytical models for dealing with unconventional attacks.³⁴² The first model is an instrument-based approach, which checks to see whether the damage caused by a new attack method could only have been previously achieved with a kinetic attack.³⁴³ The second is an effects-based approach, sometimes called a consequence-based approach, in which the attack's similarity to a kinetic

³³⁸ See WINGFIELD, *supra* note 48, at 100.

³³⁹ For instance, the United States has made several declarations regarding cyberattacks, each of which generally implies that certain cyberattacks can be treated as armed attacks, provided their scope, duration, and intensity have the same consequences as those normally associated with armed attacks. See Jensen, *supra* note 5, at 226–28; see also Dep't of Def., Office of Gen. Counsel, An Assessment of International Legal Issues, May 1999, reprinted in WINGFIELD, *supra* note 48, at 431 [hereinafter DoD Assessment] (treating cyberattacks as armed attacks when their consequences mirror those of an armed attack); Exec. Order No. 13,010, 61 Fed. Reg. 37,347 (July 15, 1996) (vowing to protect critical infrastructure against cyberattacks because their incapacitation or destruction could have a debilitating effect on U.S. defense and economic security); Exec. Order 13,321, 66 Fed. Reg. 53,063 (Oct. 16, 2001) (vowing to respond to cyberattacks against critical national infrastructure due to their potentially devastating effects on the United States).

³⁴⁰ Brown, *supra* note 51, at 187–88.

³⁴¹ See *id.* at 187. Cyberattacks can be as simple as defacing a website, or as severe as crashing another state's stock markets and keeping them shut down for some time.

³⁴² See *id.* (discussing the instrument-based and effects-based approaches); Jensen, *supra* note 5, at 223–26 (discussing the strict liability and consequence-based approaches); Horace Robertson Jr., *Self-Defense Against Computer Network Attack*, in COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 121, 134–38 (Michael N. Schmitt & Brian T. O'Donnell eds., Naval War College 2002) (discussing the consequence-based and strict liability approaches); Schmitt, *supra* note 55, at 913–17 (discussing the instrumented-based and consequence-based approaches).

³⁴³ See Brown, *supra* note 51, at 187–88; Dinstein, *supra* note 24, at 103–05. For instance, under an instrument-based approach, a cyberattack used to shut down a power grid is an armed attack, since shutting down a power grid typically requires dropping a bomb on a power station or some other kinetic use of force to incapacitate the grid. Since conventional munitions were previously required to achieve the result, under the instrument-based approach the cyberattack is therefore treated the same way.

attack is irrelevant and the focus shifts to the overall effect that the cyberattack has on a victim-state.³⁴⁴ This is the approach that the United States has adopted.³⁴⁵ The third is a strict liability approach, in which cyberattacks against CNI are automatically treated as armed attacks, due to the severe consequences that can result from disabling those systems.³⁴⁶

While these analytical models differ, the common thread between them is that the proponents of each analytical model all agree that cyberattacks can constitute an armed attack.³⁴⁷ In fact, a large number of the scenarios covered in Part III, Section B fit into the meaning of armed attack under all three models of analysis.³⁴⁸ Cyberattacks short of armed attacks would still be considered an unlawful use of force in violation of Article 2(4) of the U.N. Charter,³⁴⁹ and would have to be addressed with measures short of self-defense, such as a reprisal.³⁵⁰

³⁴⁴ See IAN BROWNLIE, *INTERNATIONAL LAW AND THE USE OF FORCE BY STATES* 362–63 (1963); WINGFIELD, *supra* note 48, at 117–30; Brown, *supra* note 51, at 187–88; Schmitt, *supra* note 55, at 1071–72; Schmitt, *supra* note 55, at 911–15. For instance, under an effects-based approach, a cyberattack that manipulated information across a state’s banking and financial institutions to seriously disrupt commerce in the state is an armed attack. While the manipulation of information does not resemble a kinetic attack, as required under an instrument-based approach, the disruptive effects that the attack had on the state’s economy is a severe enough overall consequence that it warrants treatment as an armed attack.

³⁴⁵ See DoD Assessment, *supra* note 339, at 431, 453–54.

³⁴⁶ It is important to note that this third analytical model for dealing with cyberattacks is intended to justify anticipatory self-defense before any harm actually results. Walter Gary Sharp Sr. proposes this model due to the speed with which a computer penetration can transition into a destructive attack against defense CNI. He reasons that once a penetration has occurred, an imminent threat exists with the ability to cause harm of extreme scope, duration, and intensity, thereby justifying anticipatory self-defense. See SHARP, *supra* note 24, at 129–31; *see also* Condrón, *supra* note 24, at 415–22 (discussing the need to treat cyberattacks on CNI as armed attacks); Jensen, *supra* note 5, at 228–31 (advocating changing the current *jus ad bellum* paradigm to use strict liability for cyberattacks against CNI).

³⁴⁷ See WINGFIELD, *supra* note 48, at 117–30; Brown, *supra* note 51, at 190; Dinstein, *supra* note 24, at 103–05; Schmitt, *supra* note 55, at 911–15; Robertson, *supra* note 342, at 134–38; Condrón, *supra* note 24, at 415–22; Jensen, *supra* note 5, at 228–31; KAMAL, *supra* note 22, at 76–84.

³⁴⁸ See WINGFIELD, *supra* note 48, at 117–30; Brown, *supra* note 51, at 187–88; Dinstein, *supra* note 24, at 103–05; Schmitt, *supra* note 55, at 911–15; Robertson, *supra* note 342, at 134–38; Condrón, *supra* note 24, at 415–22; Jensen, *supra* note 5, at 228–31; KAMAL, *supra* note 22, at 76–84.

³⁴⁹ See WINGFIELD, *supra* note 48, at 91–99 (discussing cyberattacks that don’t rise to the level of an armed attack). Unfortunately, trying to formulate an exact line to delineate armed cyberattacks from lesser uses of force is nearly impossible. Thus, this section shall

Of these three approaches, the effects-based approach is the best analytical model for dealing with cyberattacks. Not only does effects-based analysis account for everything that instrument-based approaches cover, but it also provides an analytical framework for situations that do not neatly equate to kinetic attacks.³⁵¹ Effects-based analysis is also superior to strict liability because responses to cyberattacks under an effects-based approach comport with internationally accepted legal norms and customs, whereas a strict liability approach may cause victim-states to violate the law of war.³⁵²

Of all of the scholars who advocate effects-based models, Michael N. Schmitt has advanced the most useful analytical framework for evaluating cyberattacks. In his seminal article, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, Michael Schmitt lays out six criteria for

advance several analytical models to help classify attacks, recognizing that it will be up to victim-states to form their view, declare whether particular cyberattacks against them are armed attacks, and defend their conclusion to the international community.

³⁵⁰ This is because at a minimum, cyberattacks are an illegal use of force. As a result, states can use reprisals to deter attackers from attacking them, and to deter sanctuary states from ignoring cyberattacks by attackers. See *supra* Part IV.E (discussing reprisals); *supra* Part V.E (discussing sanctuary states that allow attackers to act inside their borders); *infra* Parts VI.C (discussing state responsibility for failing to prevent cyberattacks).

³⁵¹ For instance, a cyberattack might shut down a system, rendering it inoperable for some time, or a cyberattack might cause an explosion at a chemical plant by tampering with the computers that controlled the feed mixture rates. The results of those attacks mirror the results of conventional armed attacks, previously only achievable through kinetic force, thus satisfying the instrument-based approach.

Unfortunately, cyberattacks can cause extreme harm without mirroring the results of conventional armed attacks. For instance, coordinated cyberattacks could bring financial markets to their knees without ever employing anything that looked remotely like a kinetic attack; altered data on a massive scale could disrupt banking, financial transactions, and the general underpinnings of the economy, sowing confusion throughout the victim-state for some time. Under an effects-based approach, the scope, duration, and intensity of this attack would equate to an armed attack, despite the fact that it was not previously only achievable through kinetic force.

³⁵² The proponents of a strict liability approach advocate automatically responding to cyberattacks on critical infrastructure with active defenses. See Condron, *supra* note 24, at 415–22; Jensen, *supra* note 5, at 228–31. However, automatically responding to cyberattacks in this manner can easily lead a victim-state to counter-attack a state with a long history of doing everything within its power to prevent cyberattacks and prosecute its attackers. Were a victim-state to respond with active defenses against a non-sanctuary state, it would violate *jus ad bellum* because there is no way to impute state responsibility to such a state, directly or indirectly, even though the cyberattack may constitute an armed attack. See *supra* Part V.C.

evaluating cyberattacks as armed attacks.³⁵³ These criteria are: severity,³⁵⁴ immediacy,³⁵⁵ directness,³⁵⁶ invasiveness,³⁵⁷ measurability,³⁵⁸ and presumptive legitimacy.³⁵⁹ Taken together, these criteria allow states to measure cyberattacks along several different axes. While no one criterion is dispositive, cyberattacks satisfy enough criteria to be characterized as armed attacks.³⁶⁰ Since their publication, Schmitt's criteria have gained traction in the legal community, with several prominent legal scholars advocating for their use.³⁶¹ Many hope that Schmitt's criteria will help bring some uniformity to state efforts to classify cyberattacks. However, until they gain wider acceptance, states are likely to classify cyberattacks differently, depending on their understanding of armed attacks as well as their conception of vital

³⁵³ Schmitt, *supra* note 55, at 913–15.

³⁵⁴ Severity looks at the scope and intensity of an attack. Analysis under this criterion would include looking at the number of people killed, size of the area attacked, and amount of property damage done. The greater the damage, the more powerful the argument becomes for treating the cyberattack as an armed attack. *See* WINGFIELD, *supra* note 48, at 124–27 (examining Schmitt's use of force analysis).

³⁵⁵ Immediacy looks at the duration of a cyberattack, as well as other timing factors. Analysis under this criterion looks at how long the cyberattack lasted, how soon its effects were felt, and how long it took for the effects to abate. The longer the duration and effects, the more it looks like an armed attack. *See id.* (examining Schmitt's use of force analysis).

³⁵⁶ Directness looks at the harm caused. If the attack was the proximate cause of the harm, it strengthens the argument that the cyberattack was an armed attack. If the harm was caused in full or in part by other parallel attacks, the weaker the argument that the cyberattack was an armed attack. *See id.* (examining Schmitt's use of force analysis).

³⁵⁷ Invasiveness looks at the locus of the attack. An invasive attack is one that physically crosses state borders, or electronically crosses borders and causes harm within the victim-state. The more invasive the cyberattack, the more it looks like an armed attack. *See id.* (examining Schmitt's use of force analysis).

³⁵⁸ Measurability tries to quantify the damage done by the cyberattack. Quantifiable harm is generally treated more seriously in the international community. The more a state can quantify the harm done to them, the more the cyberattack looks like an armed attack. Speculative harm generally makes a weak case that the cyberattack was an armed attack. *See id.* (examining Schmitt's use of force analysis).

³⁵⁹ Presumptive legitimacy focuses on state practice and the accepted norms of behavior in the international community. Actions may gain legitimacy under the law when the international community accepts certain behavior as legitimate. The less a cyberattack looks like accepted state practice, the stronger the argument that it is an illegal use of force or an armed attack. *See id.* (examining Schmitt's use of force analysis).

³⁶⁰ *See id.* at 122–29 (examining Schmitt's use of force analysis).

³⁶¹ *See* WINGFIELD, *supra* note 322, at 6–7; WINGFIELD, *supra* note 48, at 115–29; Vida Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places?*, 51 NAVAL L. REV. 132, 169–72 (2005); Robertson, Jr., *supra* note 342, at 134–38.

national interest.³⁶² Moreover, universal acceptance of Schmitt's criteria is still probably some time away.

Detractors generally criticize effects-based analysis as useful only long after a cyberattack occurs. They argue that an effects-based analysis forces states to delay their responses to the point that the state suffers preventable harm.³⁶³ More specifically, some detractors acknowledge that effects-based analysis may be useful, but advocate treating all cyberattacks on CNI as armed attacks because it is too dangerous to waste time analyzing the attack when CNI is at risk.³⁶⁴ These detractors generally advocate a strict liability approach to cyberattacks against CNI, and further advocate responding to all cyberattacks against CNI in self-defense as the only effective method to protect CNI.³⁶⁵

While the strict liability model deals adequately with threats to CNI, the model runs the risk of unlawfully escalating a situation. Effects-based analysis, on the other hand, does not require a state to delay its response until it can fully measure a cyberattack against all six of Schmitt's proposed axes. Decision-makers, at times, must make choices with imperfect information. "As a legal matter, however, the principle of anticipatory-self-defense does not, and has never, required that the threat have been genuine—only that it be perceived to be so in good faith."³⁶⁶ The imminent danger that some cyberattacks pose will force decision-makers to attempt a good faith assessment based on the facts at hand. Other cyberattacks will not be as urgent, allowing decision-makers to take time to analyze the attacks more fully. In all cases, an effects-based

³⁶² See WINGFIELD, *supra* note 322, at 8.

³⁶³ See Barkham, *supra* note 29, at 83–84.

³⁶⁴ See Condrón, *supra* note 24, at 415–22 (advocating strict liability for cyberattacks on CNI); Jensen, *supra* note 5, at 228–31 (advocating strict liability for cyberattacks on CNI).

³⁶⁵ See Condrón, *supra* note 24, at 415–22; Jensen, *supra* note 5, at 228–31.

³⁶⁶ David Rivkin Jr. et al., *War, International Law, and Sovereignty: Reevaluating the Rules of the Game in a New Century: Preemption and Law in the Twenty-First Century*, 5 CHI. J. INT'L L. 467, 496 (2005); see also Eric Jensen, *Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations?*, 18 AM. U. INT'L L. REV. 1145, 1181–82 (2003) (discussing *United States v. Wilhelm List*, XI Trials of War Criminals Before the Nuremberg Military Tribunals Under Control Council Law No. 10, 1295–96 (1950)). The legal standard for judging a military commander's decision is whether what the commander believed to be true at the time (not the actual facts) met the appropriate legal standards. This is known as the Rendulic Rule, and has been the international standard since the Nuremberg trial of General Rendulic. *Id.*

approach provides a better analytical tool to analyze an attack. Furthermore, when a threat is considered urgent, such as an attack against CNI, the potential severity and imminence of the attack may be great enough to outweigh all other considerations. Furthermore, even if cyberattacks against CNI generally constitute armed attacks, automatically responding to them in self-defense may result in the use of force against an innocent state, i.e., one that does not meet the threshold for imputing state responsibility.³⁶⁷

Classifying cyberattacks will be difficult for states to do in practice.³⁶⁸ While the initial decision to respond to cyberattacks under the law of war will have to be made by state decision-makers as a matter of policy, the actual decision to use active defenses will have to be pushed down to the system administrators who actually operate computer networks. One of the challenges states will face is translating international law into concise, understandable rules for their system administrators to follow. However, classifying cyberattacks as armed attacks or imminent armed attacks is only the first hurdle system administrators must clear before responding with active defenses. The second and equally important hurdle is establishing state responsibility for the attack.

³⁶⁷ State responsibility for cyberattacks may be established when states violate their duty to prevent cyberattacks. *See infra* Part VI.B–C.

³⁶⁸ While classifying cyberattacks will be difficult, there is no doubt that some cyberattacks will qualify as armed attacks, and should be dealt with using self-defense and anticipatory self-defense legal principles as a justification for using active defenses.

Some scholars will undoubtedly critique this conclusion. However, scholars who argue that cyberattacks cannot rise to the level of armed attacks misunderstand how states have classified unconventional attacks in the past. New attack methods frequently fall outside the accepted definitions of armed attacks. This does not mean that the attacks are not armed attacks, merely that the attacks don't fit traditional classifications. *See supra* Part VI.A (discussing the classification of new attack forms). Furthermore, scholars who argue that cyberattacks cannot rise to the level of armed attacks miss an important facet of international law—reprisals, which can be used as an alternate basis to authorize active defenses against cyberattacks. Since, at a minimum, cyberattacks are an illegal use of force, states can use reprisals to deter attackers from committing such acts in the future and to deter sanctuary states from allowing attackers to commit them. *See supra* Part IV.E (discussing reprisals); *infra* Part VI.B–C (discussing state responsibility for failing to prevent cyberattacks).

As an important sidebar, reprisals may theoretically justify using active defenses to protect non-vital computer systems. Since attacks on non-vital computer systems amount to an illegal uses of force, reprisals may provide a justification for defending those systems with active defenses (assuming the active defenses targeted non-vital systems in return). In effect, active defenses may provide a way to deter cyberattacks in general.

B. Modernizing the Approach to State Responsibility for Cyberattacks

States cannot respond to a cross-border cyberattack with force without establishing state responsibility for the attack.³⁶⁹ Historically, this meant attributing an attack to a state or its agents on the premise that a state is only responsible for its acts or the acts of those under its direct control.³⁷⁰ However, as non-state actors have attacked states with increased frequency, international law has shifted away from this traditional requirement to a model of indirect state responsibility based on a state's failure to meet its international duties.³⁷¹

This shift is especially important for cyberattacks because the prevailing view that states must treat cross-border cyberattacks as a criminal matter, rather than as a national security matter, seems to be based on the historic view of state responsibility. This limited view of state responsibility locks states into the response crisis by requiring states to attribute cyberattacks to a state or its agents,³⁷² even though the likelihood of successfully achieving such attribution is extremely remote.³⁷³ Consequently, states that subscribe to the traditional model of state responsibility will find themselves in the response crisis during a cyberattack, laboring under the false assumption that they must decide between effective, but illegal, active defenses, and the less effective, but legal, path of passive defenses and host-state criminal laws.³⁷⁴

Given the shift in the law of state responsibility, states should determine whether a cyberattack can be imputed to the state of origin, rather than trying to conclusively attribute it. Once a cyberattack is

³⁶⁹ See *supra* Part V.D.

³⁷⁰ See *supra* Part V.C.

³⁷¹ See *id.*

³⁷² See *supra* Part III.B; *supra* Part V, intro.

³⁷³ A cyberattack could be directly linked to a state under a few circumstances. Potential direct links might include a state declaration that it had made the attack; pre-attack intelligence suggesting that a state was about to make an attack; or tracing an ongoing attack to computer systems known to belong to a foreign military. Further complicating the attribution problem is that cyberterrorists and cybercriminals often hijack innocent systems and use them as zombies to initiate their cyberattacks. See *supra* Part III.A. While victim-states must try to penetrate such guises, current technology may not always allow them to do so in a timely manner. See Brown, *supra* note 51, at 201. In effect, attackers complicate the decision-making process of victim-states, who must account for these electronic disguises when trying to attribute the true identity of an attacker.

³⁷⁴ See *supra* Part III.B; *supra* Part V, intro.

imputed to a state, the legal barriers restricting self-defense disappear.³⁷⁵ States that continue to follow the prevailing view of state responsibility will unduly limit their right to use active defenses, and increase the chances of a successful cyberattack.³⁷⁶ Considering the potential catastrophic consequences of cyberattacks, states should not follow the prevailing view when the law does not require them to do so.

While neither state practice nor the publications of legal scholars support this view regarding cyberattacks yet,³⁷⁷ the accepted principles of

³⁷⁵ See *supra* Part V.C–D.

³⁷⁶ See Condrón, *supra* note 24, at 415–22; Jensen, *supra* note 5, at 228–31.

³⁷⁷ Legal scholars generally agree that states may not respond in self-defense until after an attack is attributed. See Condrón, *supra* note 24, at 415; Dinstein, *supra* note 24, at 111; Garnett & Clarke, *supra* note 13, at 478–79. As a result, state practice is currently to respond to cyberattacks with passive defenses and criminal laws. See *supra* Part II.B. However, there is a growing recognition among legal scholars that the current paradigm governing state responses to cyberattacks is inadequate to protect states and must change. See *supra* note 52. The scholars who argue against the current paradigm have tried to solve the response crisis by finding creative ways around the attribution problem. The three main proposals advanced by scholars before this article are discussed below.

One group of scholars advocates a strict liability approach to attacks against CNI. Eric Jensen first argued for this approach on the basis that attacks against CNI automatically amount to armed attacks and that attacks against them demonstrate hostile intent. See Jensen, *supra* note 5, at 236–37. Sean Condrón supports this approach arguing that international law should grant states an exception to use active defenses to protect CNI, due to the grave harm that cyberattacks against CNI can cause. See Condrón, *supra* note 24, at 415–22.

Another group of legal scholars advocates that self-defense is always a legal response to armed attacks. Their rationale is that the U.N. Charter does not subsume a state's inherent right of self-defense under CIL, which allows states to respond to armed attacks by both non-state actors and states. Thus, states can always respond to cyberattacks that amount to an armed attack regardless of who conducted it. See Barkham, *supra* note 29, at 104; Schmitt, *supra* note 55, at 933–34.

Finally, two legal scholars correctly hone in on state responsibility as the solution to the attribution problem. However, instead of tying state responsibility to a state's failure to meet its duty to prevent cyberattacks, they contend that when cyberattacks are repeatedly launched from one state against other states, the state of origin should be presumed to have involvement in the attacks. Garnett & Clarke, *supra* note 13, at 479.

Unfortunately, all three of these approaches are flawed, less likely to gain international acceptance than the approach in this article, and more likely to lead to unintended consequences with international ramifications. Scholars who advocate for first two approaches miss a critical part of the legal analysis. Namely, just because a state is under armed attack does not give it the legal authority to respond with force. It is only lawful to violate the territorial integrity of a host-state after state responsibility has been established. Were a state to respond to all cyberattacks against CNI with automated active defenses, it would result in counter-attacks against every attacking computer across the world, regardless of their state of origin. While targeting the systems of sanctuary states is an acceptable and lawful option, it is unlawful to target states that fully

customary *jus ad bellum* support imputing state responsibility for armed attacks by non-state actors when the attacks originate from a state that allows non-state actors to conduct criminal operations within their borders.³⁷⁸ States that allow non-state actors to conduct those operations breach their duty to prevent attacks against other states, and are known as sanctuary states.³⁷⁹ This principle is extremely important to the victim-states of cyberattacks because when a cyberattack originates from a sanctuary state, a victim-state may employ active defenses, thereby averting the response crisis.

It is next necessary to answer two key questions: (1) What is a state's duty to prevent cyberattacks? and (2) What must a state do (or not do) to violate its duty of prevention? The answers are the legal keys that will establish the basis for imputing state responsibility for cyberattacks, and unlock the restraints that states have placed on themselves by following the prevailing view of state responsibility.

C. The Duty to Prevent Cyberattacks

States have an affirmative duty to prevent cyberattacks from their territory against other states. This duty actually encompasses several smaller duties, to include passing stringent criminal laws, conducting vigorous investigations, prosecuting attackers, and, during the investigation and prosecution, cooperating with the victim-states of cyberattacks that originated from within their borders. These duties are the duties of all states, and, as will be shown in this section, are binding as CIL.³⁸⁰ The authority for these duties comes from all three sources of

participate in international efforts to secure cyberspace. Furthermore, counter-attacks against those states could be seen as acts of war.

³⁷⁸ See *supra* Part V.C (reviewing the principles of state responsibility).

³⁷⁹ See *supra* Part V.B (reviewing the duty to prevent non-state actors from using a state's territory to commit criminal acts against another state); *supra* Part V.D (reviewing sanctuary states and the legality of holding them responsible for the actions of those non-state actors).

³⁸⁰ For a discussion and definition of CIL, see *supra* notes 179 and 283. The other principal source of international law is international agreements. *Id.* § 102. The third and somewhat ancillary source of international law is the general principles of law common to the major legal systems of the world; however, this is infrequently used as a source of international law. An example of a general legal principle is the prohibition on torture in most domestic legal systems. *Id.*

These definitions roughly mirror the sources of international law found in the Statute of the ICJ. The Statute of the ICJ lists four sources of international law, the first three of

CIL—international conventions, international custom, and the general principles of law common to civilized nations, as also evidenced by judicial decisions and the teachings of the most highly qualified international legal scholars.

1. *Support from International Conventions*

The only international treaty directly on point is the European Convention on Cybercrime. While the treaty is only a regional agreement, it influences CIL because of the importance of the states that have ratified it under the specially-affected-state doctrine.³⁸¹

which mirror these sources of international law, and then uses judicial opinions and the publications of scholars as a subsidiary means for determining the law. Furthermore, the statute's description of international custom roughly mirrors the Restatement's description of CIL. See Statute of the International Court of Justice art. 38(1), June 26, 1945, 59 Stat. 1055, 1060 (1945).

³⁸¹ Customary international law does not require state practice to be universal. General practices can satisfy the requirements of customary international law. State practices become customary international law when the practice is extensive and representative. "That is to say, it is not simply a question of how many States participate in the practice, but also *which* States." Jean-Marie Henckaerts, *Customary International Humanitarian Law Study: A Contribution to the Understanding and Respect for the Rule of Law in Armed Conflict*, in *THE LAW OF WAR IN THE 21ST CENTURY: WEAPONRY AND THE USE OF FORCE* 37, 42 (Anthony M. Helm ed., Naval War College 2006) (emphasis added). The specially-affected-state doctrine comes into play when states whose interests are specially affected by a practice all follow the practice, and the practice becomes CIL even if the majority of states do not participate, as long as the majority acquiesces to the practice. Likewise, if the majority of states declare something to be CIL and the specially affected states do not accept the practice, it cannot become CIL. *Id.* at 42–43. In other words, states whose interests are particularly impacted by a particular state practice are specially-affected-states, and their practices carry more weight in contributing to CIL about that practice. Yoram Dinstein, *The ICRC Customary International Law Study*, in *THE LAW OF WAR IN THE 21ST CENTURY: WEAPONRY AND THE USE OF FORCE* 99, 109 (Anthony M. Helm ed., Naval War College 2006). The specially-affected-state doctrine was developed by the ICJ in *North Sea Continental Shelf*. *North Sea Continental Shelf (F.R.G. v. Den.; F.R.G. v. Neth.)*, 1969 I.C.J. 3, 43 (Feb. 20).

To date, twenty-six states have ratified the Convention on Cybercrime, the majority of which are major western powers, three of which hold permanent Security Council seats, and five of which place among the twenty states with the most Internet users in the world—France, Germany, Italy, the United Kingdom, and the United States. Together, these five states account for twenty-five percent of the Internet users in the world. Furthermore, while not yet parties to the treaty, Canada, Japan, Spain, and Poland are signatories to it and are expected to ratify it soon. These four states are among the remaining twenty states with the most Internet users in the world, and their ratification would greatly move state practice to the standards set forth in the convention. See Council of Europe, Convention on Cybercrime, Chart of Signatures and Ratifications,

Furthermore, it demonstrates state recognition of both the need to criminalize cyberattacks, and the duty of states to prevent their territory from being used by non-state actors to conduct cyberattacks against other states.³⁸² Significantly, the Convention also recognizes that cyberattacks cannot be interdicted during the middle of an attack, and that the only way to prevent them is through aggressive law enforcement, coupled with state cooperation.³⁸³

International treaties to criminalize terrorism provide further support, albeit indirectly, for the duty to prevent cyberattacks. The international community recognizes terrorism as a threat to international peace and security, but cannot agree on a definition of it.³⁸⁴ As a result, states have adopted the approach of outlawing specific terrorist acts each time terrorists adopt new attack methods, rather than outlawing terrorism itself.³⁸⁵ These treaties impose several common requirements on states

<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=18/06/04&CL=ENG> (listing the forty-six signatories and twenty-six parties to the Convention on Cybercrime) (last visited Sept. 2, 2009); Top 20 Countries with the Highest Number of Internet Users, <http://www.internetworldstats.com/top20.htm> (last visited Sept. 2, 2009).

³⁸² The Convention on Cybercrime requires its signatories to establish criminal offenses for almost every conceivable type of cyberattack under their domestic laws. *See* Convention on Cybercrime, *supra* note 22, arts. 2–11, at 284–87. It also recognizes the importance of prosecuting attackers, demonstrated by its requirement for states to extend their jurisdiction over any cyberattacks conducted from within their territory, or conducted by their citizens regardless of their location at the time of attack. *See id.* art. 22, at 291–92. Finally, the convention recognizes the importance of state cooperation to hunt down attackers and bring them to justice; requiring states to cooperate with each other and provide “mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences.” *See id.* arts. 23–25, at 292–93.

³⁸³ *See* KAMAL, *supra* note 22, at 71.

³⁸⁴ Pierre-Marie Dupuy, *State Sponsors of Terrorism: International Responsibility*, in *ENFORCING INTERNATIONAL LAW NORMS AGAINST TERRORISM* 3, 4–6 (Andrea Bianchi ed., 2004).

One reason why it has been difficult to secure a universally accepted definition of terrorism has been that some States, primarily from the developing world, have sought to resist condemnation of practices and activities which they may have resorted to in their acquiring of independence, particularly during decolonization.

Gannett & Clarke, *supra* note 13, at 466.

³⁸⁵ Dupuy, *supra* note 384, at 4–6; Gannett & Clarke, *supra* note 13, at 466. These treaties include the 1963 Tokyo Convention on Offences and Certain Other Acts Committed on Board Aircraft, the 1970 Hague Convention for the Suppression of

with regard to terrorist attack methods, such as taking all practicable measures for the purpose of preventing these attacks, criminalizing the attacks, submitting cases to competent authorities for prosecution, and forcing states to cooperate with each other throughout the criminal proceedings.³⁸⁶ While these treaties do not address cyberattacks, the principles contained in them help influence state requirements under CIL with regard to terrorism. Since there is growing evidence that cyberattacks will soon be a weapon of choice for terrorists,³⁸⁷ states should refer to the common principles found in these treaties as *opinio juris* when cyberattacks are used as a terrorist weapon.

2. Support from State Practice

State treatment of cyberattacks under their criminal laws also evidence recognition of the duty to prevent cyberattacks under CIL. Numerous states criminalize and prosecute cyberattacks as a way to deter attackers from conducting them, on the basis that vigorous law enforcement is the only way to protect and prevent harm to their

Unlawful Seizure of Aircraft, the 1971 Montreal Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, the 1979 International Convention Against the Taking of Hostages, the 1988 Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, the 1988 Montreal Protocol on the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, the 1997 International Convention for the Suppression of Terrorist Bombings, the 1999 International Convention for the Suppression of the Financing of Terrorism, and the 2005 International Convention for the Suppression of Acts of Nuclear Terrorism. *See* Dupuy, *supra* note 384, at 4–6 (using several of these as examples of treaties that outlawed particular terrorist attack methods); Gannett & Clarke, *supra* note 13, at 466 (using several of these as examples of treaties that outlawed particular terrorist attack methods).

³⁸⁶ *See generally* Hague Convention for the Suppression of Unlawful Seizure of Aircraft, *done* Dec. 16, 1970, 22 U.S.T. 1641, T.I.A.S. No. 7192; Montreal Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, *done* Sept. 23, 1971, 24 U.S.T. 564, T.I.A.S. No. 7570; International Convention Against the Taking of Hostages, *opened for signature* Dec. 18, 1979, 18 I.L.M. 1456; Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, *done* Mar. 10, 1988, 1678 U.N.T.S. 221, 27 I.L.M. 668; International Convention for the Suppression of Terrorist Bombings, *opened for signature* Jan. 12, 1998, 37 I.L.M. 249; International Convention for the Suppression of the Financing of Terrorism, *opened for signature* Jan. 10, 2000, 39 I.L.M. 270; International Convention for the Suppression of Acts of Nuclear Terrorism, *opened for signature* Sept. 14, 2005, 44 I.L.M. 815.

³⁸⁷ Gannett & Clarke, *supra* note 13, at 467; ROLLINS & WILSON, *supra* note 15, at CRS-1.

computer systems.³⁸⁸ This lends credence to the notion that, unlike a conventional attack which can be stopped after detection, cyberattacks can only be stopped by establishing *ex ante* barriers that attackers are fearful of crossing. Furthermore, these practices demonstrate a growing recognition among states that cyberattacks must be stopped, and that the way to do so is through vigorous law enforcement.

State responses to transnational terrorist attacks further support recognition of a duty to prevent cyberattacks under CIL. After the 9/11 terrorist attacks, states across the world condemned terrorism as a threat to international peace and security, and provided various forms of support to the United States in its war against al Qaeda.³⁸⁹ Ensuring that terrorism will forever be legally recognized as a threat to international peace and security, the Security Council passed Resolution 1373, which reaffirmed that acts of international terrorism were threats to international peace and security and called on states to work together to prevent and suppress terrorism.³⁹⁰ The resolution further directed states to “[r]efrain from providing any form of support” to terrorists through act or omission, to “[d]eny safe haven” to those who commit terrorist acts, and “[a]fford one another the greatest measure of assistance in connection with criminal investigations . . . [or] proceedings” related to terrorism.³⁹¹

While the international community’s response to terrorism does not directly define CIL regarding cyberattacks, it is persuasive on several fronts. First, it shows that states have a duty to prevent threats to international peace and security. Second, it demonstrates that passive acquiescence to threats to international peace and security will not be tolerated. Finally, it demonstrates that states must work together to prevent and suppress threats to international peace and security. Because states are growing more dependent on computer systems connected to the Internet,³⁹² and cyberattacks are increasing in both frequency and

³⁸⁸ See KAMAL, *supra* note 22, at 17–22, 40–42, 175–184 (discussing the criminal laws of Australia, Austria, Belgium, Brazil, Canada, Denmark, France, Germany, India, Japan, the Netherlands, South Africa, the United States, and the United Kingdom). Many other states have criminalized computer crimes, such as the unauthorized access or alteration of data, or computer sabotage, but those laws shall not be covered in this article. Garnett & Clarke, *supra* note 13, at 471.

³⁸⁹ See *supra* Part V.A.

³⁹⁰ S.C. Res. 1373, U.N. Doc. S/RES/1373 (Sept. 28, 2001).

³⁹¹ *Id.*, ¶ 1.

³⁹² See *supra* Part II, intro; Part III.B.

potency,³⁹³ cyberattacks are a growing threat to international peace and security. The more cyberattacks resemble terrorism, the more easily they will fit into the paradigm constructed to deal with transnational terrorism. However, no matter their purpose, cyberattacks represent a threat to international peace and security, and should be dealt with like other recognized transnational threats.

Numerous U.N. declarations about international crime also support recognizing the duty to prevent cyberattacks. These declarations urge states to take affirmative steps to prevent non-state actors from using their territory to commit acts that cause civil strife in another state.³⁹⁴ Furthermore, these declarations bolster the duty of states to cooperate with one another to eliminate transnational crime, which supports the duty to cooperate with victim-states during the criminal investigation and prosecution of cyberattacks.³⁹⁵

³⁹³ See Part II, intro; Part III.B.

³⁹⁴ The 1970 Declaration on Friendly Relations urges states to “refrain from . . . acquiescing [to] organized activities within [their] territory directed towards the commission of [civil strife or terrorism in another state].” G.A. Res. 2625, *supra* note 277, ¶ 1. The 2000 Vienna Declaration on Crime and Justice states that “We [must] commit ourselves to working towards enhancing our ability to prevent, investigate and prosecute high-technology and computer-related crime.” 2000 Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-First Century, G.A. Res. 55/59, Annex, ¶ 18, U.N. Doc. A/RES/55/59/Annex (Jan.17, 2001). The 2001 Draft Articles of State Responsibility require states to affirmatively take action to uphold their international duties to other states, including those arising from CIL, and declare that when states fail to act, they may be held indirectly responsible for such inaction. Draft Articles on the Responsibility of States for Internationally Wrongful Acts, U.N. Doc. A/CN.4/L.602/Rev. 1 (2001).

³⁹⁵ The 1970 Declaration on Friendly Relations notes that “[s]tates have a duty to cooperate with one another . . . in order to maintain international peace and security.” G.A. Res. 2625, *supra* note 277, ¶ 1. The 2004 Report of the High-Panel on Threats, Challenges and Change recognizes the growing threat of organized transnational crime as a threat to international peace and security, stating that “today, more than ever before, threats are interrelated and a threat to one is a threat to all.” The Secretary-General, *Report of the High-Panel on Threats, Challenges and Change*, ¶ 17, delivered to the General Assembly, U.N. Doc A/59/565 (Dec. 2, 2004). It goes on to further state:

No State, no matter how powerful, can by its own efforts alone make itself invulnerable to today’s threats. Every State requires the cooperation of other States to make itself secure. It is in every State’s interest, accordingly, to cooperate with other States to address their most pressing threats, because doing so will maximize the chances of reciprocal cooperation to address its own threat priorities.

Id. ¶ 24.

Focusing specifically on cyberattacks, states have made declarations themselves, and used the U.N. General Assembly to make numerous declarations about the importance of preventing cyberattacks. For instance, the U.N. General Assembly has called on states to criminalize cyberattacks,³⁹⁶ and to deny their territory from being used as a safe haven to conduct cyberattacks through state practice.³⁹⁷ The General Assembly has also called on states to cooperate with each other during the investigation and prosecution of international cyberattacks.³⁹⁸ Even China has said it will “take firm and effective action to prevent all hacking attacks that threaten computer systems.”³⁹⁹ Furthermore, states are starting to recognize the threat that cyberattacks pose to international peace and security, with some states and the General Assembly directly recognizing cyberattacks as a danger to international peace and security.⁴⁰⁰ These declarations all recognize that the duty of states to

³⁹⁶ G.A. Res. 45/121, ¶ 3, U.N. Doc. A/RES/45/121 (Dec. 14, 1990) (embracing the principles adopted by the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, and inviting states to follow them); G.A. Res. 55/63, ¶ 1, U.N. Doc. A/RES/55/63 (Jan. 22, 2001); *see also* Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Cuba, Aug. 27–Sept. 7, 1990, *report prepared by the Secretariat*, at 140–43, U.N. Doc. A/CONF.144/28/Rev.1 (1991).

³⁹⁷ G.A. Res. 55/63, *supra* note 396, ¶ 1.

³⁹⁸ G.A. Res. 45/121, *supra* note 396, ¶ 3 (embracing the principles adopted by the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, and inviting states to follow them); G.A. Res. 55/63, *supra* note 396, ¶ 1; *see also* Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Cuba, Aug. 27–Sept. 7, 1990, *report prepared by the Secretariat*, at 140–43, U.N. Doc. A/CONF.144/28/Rev.1 (1991).

³⁹⁹ McGregor & Williamson, *supra* note 43 (quoting China’s Premier Wen Jiabao’s pledge to prevent international cyberattacks in response to allegations that China is ignoring international cyberattacks).

⁴⁰⁰ *See* CYBERSPACE NAT’L STRATEGY, *supra* note 10 (noting the threat that cyberattacks pose to international peace and security); Convention on Cybercrime, *supra* note 22 (recognizing cyberattacks as a threat to international peace and security, and calling on states to work together to end the cyberthreat); Huw Jones, *Estonia Calls for EU Law to Combat Cyberattacks*, REUTERS, Mar. 12, 2008, <http://www.reuters.com/article/reutersEdge/idUSL1164404620080312> (reporting Estonia’s call to fight cyberattacks as a threat to international peace and security); G.A. Res. 53/70, U.N. Doc. A/RES/53/70 (Jan. 4, 1999) (expressing concern that information technology can be used to disrupt international stability and noting that it is necessary for states to stop information technology from being used for criminal or terrorist purposes); G.A. Res. 54/49, ¶ 2, U.N. Doc. A/RES/54/49 (Dec. 23, 1999) (recommending states develop international principles to combat cybercrime and cyberterrorism); G.A. Res. 55/28, U.N. Doc. A/RES/55/28 (Dec. 20, 2000) (urging states to cooperate to eliminate the misuse of information technology); G.A. Res. 56/19, U.N. Doc. A/RES/56/19 (Jan. 7, 2002) (reaffirming the conclusions of General Assembly Resolutions 53/70, 54/49, and 55/28); G.A. Res. 56/121, U.N. Doc. A/RES/56/121 (Jan. 23, 2002) (urging states to continue to

prevent cyberattacks as a matter of CIL also includes the following lesser duties: passing stringent criminal laws, vigorously investigating cyberattacks, prosecuting attackers, and having the host-State and victim-state cooperate during the investigation and prosecution of cases.

3. Support from the General Principles of Law

The general principles of law common to civilized nations also support recognition of a duty to prevent cyberattacks. It is a well-established principle under the domestic laws of most states that individuals should be responsible for acts or omissions that have a causal link to harm suffered by another individual.⁴⁰¹ While international law is not obligated to follow the domestic laws of states,⁴⁰² international law may be “derived from the general principles common to the major legal

work to eliminate the criminal misuse of information technology); G.A. Res. 57/53, U.N. Doc. A/RES/57/53 (Dec. 30, 2002); G.A. Res. 57/239, ¶¶ 1–5, U.N. Doc. A/RES/57/239 (Jan. 31, 2003) (calling on states to “create a global culture of cybersecurity”); G.A. Res. 58/32, U.N. Doc. A/RES/58/32 (Dec. 18, 2003); G.A. Res. 58/199, ¶ 1–6, U.N. Doc. A/RES/58/199 (Jan. 30, 2004) (recognizing the threat that cyberattacks pose to CNI; recognizing that protecting CNI requires international cooperation and law enforcement; and calling on states to create a global culture of cybersecurity); G.A. Res. 59/61, U.N. Doc. A/RES/59/61 (Dec. 16, 2004); G.A. Res. 59/220, ¶ 4, U.N. Doc. A/RES/59/220 (Feb. 11, 2005) (endorsing the Declaration of Principles adopted at the 2003 World Summit on the Information Society, *available at* <http://www.itu.int/wsis/docs/geneva/official/dop.html>, which recognizes the need for states to prevent information technology from being used for criminal or terrorist purposes); G.A. Res. 60/45, U.N. Doc. A/RES/60/45 (Jan. 6, 2006); G.A. Res. 60/252, ¶ 8, U.N. Doc. A/RES/60/252 (Apr. 27, 2006) (reiterating the need for states’ cooperation); G.A. Res. 61/54, U.N. Doc. A/RES/61/54 (Dec. 19, 2006); *see also* G.A. Res. 51/210, ¶ 3, U.N. Doc. A/RES/51/210 (Dec. 16, 1996) (calling upon states “[t]o note the risk of terrorists using electronic or wire communications systems and networks to carry out criminal acts and the need to find means, consistent with national law, to prevent such criminality and to promote cooperation where appropriate”); S.C. Res. 1373, *supra* note 390, ¶ 3 (calling upon states to cooperate and share information about the “use of communications technologies by terrorist groups”).

⁴⁰¹ BECKER, *supra* note 304, at 285–86. Causation is applied differently by states. Some states use a “but for” test, looking to see whether the harm in question “would have occurred were it not for the conduct in question.” *Id.* at 291. Other states use a “proximate cause” test, looking to see whether harm was reasonably foreseeable as a result of an individual’s actions or omissions. *Id.* Omissions are generally treated the same as acts. So, for instance, if a parent chose not to feed a child, the parent would still bear responsibility for the harm to the child because the failure to act caused harm when it was the parent’s duty to prevent such harm. *Id.* at 294–97.

⁴⁰² *Id.* at 287.

systems of the world.”⁴⁰³ Most states use causation as a principle for establishing individual responsibility, strengthening the idea that a state’s responsibility should also be based on causation. Thus, if a state failed to pass stringent criminal laws, did not investigate international cyberattacks, or did not prosecute attackers, it should be held responsible for international cyberattacks against another state because its omission helped create a safe haven for attackers to attack other states. Furthermore, the general duty to prevent attacks already accounts for causation to some degree,⁴⁰⁴ which supports using causation analogies from domestic laws when interpreting the customary duty to prevent cyberattacks.

4. Support from Judicial Opinions

Finally, judicial opinions further support recognition of a state’s affirmative duty to prevent cyberattacks from its territory against other states. In *Tellini*, a special committee of jurists held that a state may be held responsible for the criminal acts of non-state actors when it “neglect[s] to take all reasonable measures for the prevention of the crime and pursuit, arrest and bringing to justice of the criminal.”⁴⁰⁵ In *S.S. Lotus*, the Permanent Court of International Justice (ICJ) held that “a state is bound to use due diligence to prevent the commission within its dominions of criminal acts against another nation or its people.”⁴⁰⁶ In *Corfu Channel*, the ICJ held that states have a duty “not to allow knowingly its territory to be used for acts contrary to the rights of other states.”⁴⁰⁷ While these are older cases, their principles still stand for and support the notion that states have a duty to prevent their territory from

⁴⁰³ RESTATEMENT, *supra* note 283, § 102.

⁴⁰⁴ For instance, in the *Corfu Channel Case*, the ICJ held that Albania was responsible for notifying British ships of a minefield in their waters, even though the mines were laid by non-state actors, because it was unreasonable to assume that Albania did not know of their presence (even though Albania claimed not to know of them) and because states have a duty to prevent their territory from being used to harm other states when it is within their power to do so. In effect, Albania could have prevented the British ships from hitting the mines, but their failure to act caused the British ships harm. See *Corfu Channel Case (Merits)*, 1949 I.C.J. 4 (Apr. 9). *But see* BECKER, *supra* note 304, at 287–89 (noting that some scholars argue that international law and domestic law are so dissimilar that comparisons between the two are useless).

⁴⁰⁵ *Tellini case*, 4 League of Nations O.J. 524 (1924).

⁴⁰⁶ See *S.S. Lotus (Fr. v. Turk.)* 1927 P.C.I.J. (ser. A) No. 10, at 4, 88 (Moore, J., dissenting).

⁴⁰⁷ *Corfu Channel Case (Merits)*, 1949 I.C.J. 4, 22 (Apr. 9).

being used to commit criminal acts against another state, as well as a duty to pursue, arrest, and bring to justice criminals who have conducted cross-border attacks on other states.

5. *Further Defining a State's Duty to Prevent Cyberattacks*

A state's duty to prevent cyberattacks should not be based on a state's knowledge of a particular cyberattack before it occurs, but rather on its actions to prevent cyberattacks in general. Cyberattacks are extremely difficult for host-states to detect prior to the commission of a specific attack⁴⁰⁸ and are often committed by individuals or groups who are not even on a state's radar. However, just because cyberattacks are difficult to prevent does not mean that states cannot breach their duty to prevent them. Stringent criminal laws and vigorous law enforcement will deter cyberattacks.⁴⁰⁹ States that do not enact such laws fail to live up to their duty to prevent cyberattacks. Likewise, even when a state has stringent criminal laws, if it looks the other way when cyberattacks are conducted against rival states, it effectively breaches its duty to prevent cyberattacks; its unwillingness to do anything to stop the cyberattacks is as if it had approved them.⁴¹⁰ A state's passiveness and indifference toward cyberattacks make it a sanctuary state from where attackers can safely operate. When viewed in this light, a state can be held indirectly responsible for cyberattacks under the established principles of CIL.

D. *Becoming a Sanctuary State: Practices that Lead to State Responsibility*

Determining if a state is acting as a sanctuary state is extremely fact dependent. When considering this question, victim-states must look at the host-state's criminal laws, law enforcement practices, and track

⁴⁰⁸ See Naraine, *supra* note 167 (referencing Secretary of Homeland Security Michael Chertoff's speech on the vulnerability of federal computer systems).

⁴⁰⁹ See COLARIK, *supra* note 6, at 39; KAMAL, *supra* note 22, at 176.

⁴¹⁰ A state that is unable to fulfill its duty to prevent cyberattacks due to a lack of technical expertise should be viewed in compliance with its duty to prevent when it accepts technical assistance from the victim-state to hunt down the attackers. Cooperating in law enforcement efforts demonstrates the state's willingness to prevent cyberattacks. Conversely, a state that lacks technical expertise, but refuses to accept outside assistance, would be viewed as unwilling to take the necessary steps to bring attackers to justice.

record of cooperating with the victim-states of cyberattacks that previously originated from inside its borders. In effect, host-states will be judged on their efforts to catch and prosecute attackers who have committed cyberattacks, which is probably the only way that states can deter and prevent future attacks. Since victim-states will end up judging whether a host-state has lived up to its international duties, host-states must cooperate with victim-states to ensure transparency. Cooperation will necessarily entail a host-state showing its criminal investigations to a victim-state, so victim-states can correctly judge the host-state's actions. Furthermore, when a host-state lacks the technical capacity to track down an attacker, international law should require it to work together with law enforcement officials from the victim-state to jointly track down the attackers.⁴¹¹ These two measures will prevent host-states from being perceived as uncooperative and complicit in the use of their networks for attacks against other states. States that deny involvement in a cyberattack, but refuse to open their investigative records to the victim-state, cannot expect to be treated as a state living up to its international duties. In effect, host-states that refuse to cooperate with victim-states are unwilling to prevent cyberattacks and have declared themselves a sanctuary state.

Once a host-state demonstrates, by inaction, that it is a sanctuary state, other states can impute responsibility to it. At that point, the host-state becomes liable for the cyberattack that triggered an initial call for investigation, as well as for all future cyberattacks originating from it. This opens the door to a victim-state to use active defenses against the computer servers in that state during a cyberattack.

VII. The Choice to Use Active Defenses: Moving Towards a Workable Approach

While this article urges states to use active defenses to protect their computer networks, states that use them will find themselves confronted with difficult legal decisions. Technological limitations will place states in a position where a timely decision to use active defenses requires

⁴¹¹ This position is supported by numerous U.N. General Assembly Resolutions, the European Convention on Cybercrime, and other U.N. documents, which all generally urge states to cooperate in investigating and prosecuting the criminal misuse of information technologies. *See supra* notes 382, 394–98, 400 and accompanying text; UNITED NATIONS MANUAL ON THE PREVENTION AND CONTROL OF COMPUTER RELATED CRIME ¶ 268–73 (1995), available at <http://www.uncjin.org/Documents/irpc4344.pdf>.

states to decide to use them with imperfect knowledge. Since forcible responses to cyberattacks must comply with both principal areas of the law of war—*jus ad bellum* and *jus in bello*⁴¹²—the decision to use active defenses raises several other questions of law resulting from these technical limitations. From a practical standpoint, this will affect state decision-making at the highest and lowest levels of government. State policymakers will need to account for these limitations when setting state policy, while state system administrators will need to account for these limitations when responding to actual cyberattacks.

This part will analyze these issues. First, it will analyze the technological limitations that are likely to affect state *jus ad bellum* analysis. Next, it will move on to *jus in bello* issues. *Jus in bello* analysis will begin with the decision to use force, analyzing why active defenses are the most appropriate forceful response to cyberattacks. The *jus in bello* analysis will conclude with the impact that technological limitations are likely to have on state decisions to use force. Once complete, it will be clear that active defenses are a viable way for states to protect themselves despite the fact that technological limitations complicate state decision-making.

A. Technological Limitations and *Jus ad Bellum* Analysis

While cyberattack analysis is greatly simplified by looking at whether a state of origin has violated its duty to prevent an attack, rather than having to attribute it, states are still likely to find cyberattacks difficult to deal with in practice. *Jus ad bellum* requires states to carefully analyze a cyberattack and ensure that (1) the attack constitutes an armed attack or imminent armed attack; and (2) the attack originates from a sanctuary state. Both of these conditions must exist before a state can lawfully respond with active defenses under *jus ad bellum*.

Cyberattack analysis will be conducted by system administrators, whose position puts them at the forefront of computer defense. System administrators can use various computer programs to facilitate their analysis. Automated detection and warning programs can help detect intrusions, classify attacks, and flag intrusions for administrator action.⁴¹³

⁴¹² See *supra* notes 170–71 and accompanying text.

⁴¹³ See Naraine, *supra* note 167 (referencing former Secretary of Homeland Security Michael Chertoff's discussion of the Federal Government's computer system defenses).

Automated or administrator-operated trace programs can trace attacks back to their point of origin.⁴¹⁴ These programs can help system administrators to classify cyberattacks as armed attacks or lesser uses of force, and evaluate whether attacks originate from a state previously declared a sanctuary state. When attacks meet the appropriate legal thresholds, system administrators may use active defenses to protect their networks.⁴¹⁵

Unfortunately, technological limitations on attack detection, attack classification, and attack traces are likely to further complicate state decision-making during cyberattack analysis. Ideally, attacks would be easy to detect, classify, and trace. Unfortunately, this is not the case. This section will analyze the technological limits of these programs and explore their likely impact on state decision-makers and system administrators.

1. Limitations on Attack Detection

While early detection and warning programs can help catch cyberattacks before they reach their culminating point, even the best programs are unable to detect all cyberattacks.⁴¹⁶ As a result, cyberattacks are bound to harm states. From a legal perspective, the failure to catch an attack until after its completion has both an upside and a downside. On the upside, states would gain the luxury of time to evaluate an attack, since the threat of danger will have already passed. On the downside, tracing an attack back to its source becomes more difficult the further removed the trace becomes from the time of attack.⁴¹⁷

⁴¹⁴ See Wheeler & Larsen, *supra* note 158, at 23–24 (discussing the use of automated tracer programs to find the originating point of a cyberattack). See generally Wheeler & Larsen, *supra* note 158, for a technical discussion on tracing cyberattacks back to their point of origin.

⁴¹⁵ See *supra* Part IV.C–D (discussing the thresholds for armed attacks and imminent armed attacks); *supra* Part VI.A (discussing cyberattacks as armed attacks); *supra* Part VI.B–C (discussing state responsibility for cyberattacks when states violate their duty to prevent them); see also Wheeler & Larsen, *supra* note 158, at 24 (noting that the U.S. Department of Defense has already developed these capabilities, but has been restricted from using them by the U.S. Department of Justice due to the legal issues that active defenses raise).

⁴¹⁶ See Naraine, *supra* note 167 (quoting former Secretary of Homeland Security Michael Chertoff).

⁴¹⁷ See Wheeler & Larsen, *supra* note 158, at 51–52. An ongoing attack is the easiest to trace, allowing states to trace an electronic pathway back to the source. *Id.* at 9–42, 51–

Furthermore, even when it turns out that an armed cyberattack originates from a sanctuary state, state decision-makers would need to think long and hard about using active defenses as a matter of law and policy. The longer it takes to detect an attack, the less compelling the need for states to use active defenses, especially when the attack seems truly complete. On the other hand, when an attack that has reached completion is seen as part of a series of ongoing attacks, the need to use active defenses to deter future attacks is more compelling.⁴¹⁸

2. *Limitations on Attack Classification*

Early detection and warning programs will detect many cyberattacks mid-attack. However, detecting an attack before its culmination makes it harder to classify. Naturally, a system administrator will immediately attempt to shut down a cyberattack with passive defenses as soon as it is detected. However, that is not the full extent of his job. The system administrator must also assess the damage that has been done, as well as any likely future damage, so that an informed decision can be made about whether to use active defenses.⁴¹⁹

When an ongoing cyberattack has already caused severe, invasive, and measurable damage, it can safely be classified as an armed attack,

52. Completed attacks are much more difficult to trace because the electronic pathways no longer exist and data may have been destroyed. In addition, piercing the shield that zombies or other intermediaries (if any) had created for the true attacker may be a challenge. *Id.* at 51–52.

⁴¹⁸ The more an attack is seen as part of a series of attacks originating from the host-state, the more extensive a victim-state's response can be. The permissible response will be highly fact dependent based on behavioral trends of the host-state and intelligence about the host-state's intentions. *See supra* Part IV.C–D. Thus, cyberattacks from sanctuary states are more likely to be seen as part of an ongoing series of attacks, even when the attacks are actually committed by different attackers within the state, because the sanctuary states have already demonstrated that they allow attacks from within their territory. *See supra* Part VI.B–D.

⁴¹⁹ System administrators must determine whether the attack meets the threshold of an armed attack. To do so, they would need to weigh (1) the potential harm that could occur from the attack to ensure that it was an armed attack; (2) the likelihood of fending off the attack with purely defensive measures, to ensure that active defenses were necessary; and (3) the imminency of such harm, since active defenses may not be employed until delaying their use starts to endanger the state. These decisions will, no doubt, be based on rules promulgated by the victim-state before the attack ever occurs. These rules would simplify the legal framework into a set of rules more easily understood by the layperson, similar to the rules of engagement that military personnel follow.

even though it is still ongoing.⁴²⁰ On the other hand, when an attack has not caused severe, invasive, or measurable damage, a system administrator will need to look at the immediacy of future harm to determine whether the attack should be classified as an imminent armed attack.⁴²¹ Given the lightning speeds with which computer codes can execute, this decision will be very difficult to make, since delaying the use of active defenses increases the likelihood of harm to a state.⁴²²

The limitations on attack classification should give system administrators pause before deciding to use active defenses in anticipatory self-defense. While it is lawful to make a decision based on their best analysis of the facts,⁴²³ such determinations will be highly speculative due to the shadowy nature of cyberattacks. Most likely, when a computer intrusion is detected, the purpose of the attack will be difficult to discern without dissecting a program's code or reviewing the

⁴²⁰ See *supra* Part VI.A. The 2007 cyberattack against Estonia is a good example of an ongoing attack that had risen to the level of an armed attack when it was detected. That attack no doubt rose to the level of an armed attack early in the process, disrupting the ability of the Estonian government to govern; yet the attacks continued for several weeks afterwards, further damaging Estonian systems far beyond the damage at the point of detection. See *supra* Part I, introduction.

Furthermore, when evaluating a cyberattack as an armed attack, states need to determine whether the cyberattack is part of a series of coordinated cyberattacks against a state. When this happens, it is possible for the collective effect of the attacks to rise to the level of an armed attack, even though none of the individual attacks did so. In this type of situation, the collected cyberattacks against non-critical infrastructure can be considered an armed attack. See *supra* Part VI.A. This would require analysis at a higher national level than the particular institution being individually attacked. The Cyber Warning and Information Network and National Cyber Alert System is an example of such an effort in the United States. See WILSON, *supra* note 15, at CRS-31 to CRS-32. The 2007 cyberattacks against Estonia were an example of a coordinated set of cyberattacks that collectively rose to the level of an armed attack. While some of the attacks on Estonia were against critical infrastructure, and might have been considered armed attacks singly, the collective effect was much greater than the damage done in any of the individual attacks, and certainly pushed those cyberattacks to the level of armed force. See *supra* Part II, introduction.

⁴²¹ See *supra* Part VI.A.

⁴²² System administrators can attempt to quarantine and analyze malicious code to buy time. However, this is not always possible. Furthermore, unauthorized remote penetrations cannot be quarantined or slowed down. For these cyberattacks, system administrators will need to sever the connection and end the attack, which may not always be possible. However, all of this takes time, which is why it is easier to automate classification and trace programs to uncover the basic facts about a cyberattack and its point of origin, flag the attack for a system administrator's attention, and have active defenses at the ready. See *supra* Part III.C.

⁴²³ See *supra* note 366 and accompanying text.

audit logs of an attacker's activity.⁴²⁴ Furthermore, the speed with which cyberattacks execute will force system administrators to make their best guess, even though they will probably be missing critical information. Given the speculative nature of any such calculus,⁴²⁵ as a matter of policy, state decision-makers may want to direct their system administrators to respond to cyberattacks in anticipatory self-defense only as an act of last resort, to prevent an escalation of hostilities between states.

3. *Limitations on Attack Traces*

Cyberattacks are frequently conducted through intermediate computer systems to disguise the true identity of an attacker.⁴²⁶ While trace programs are capable of penetrating intermediate disguises back to their electronic source, their success rate is not perfect.⁴²⁷ Thus, trace programs run the risk of incorrectly identifying the true source of an attack. This limitation creates an apparent problem because an attack could be incorrectly perceived as coming from a state that is not the actual state of origin. However, the problem is not as big as it appears. State responsibility should still be judged on the facts at hand, even if it results in misattribution. First, as long as a state assesses an attack to the

⁴²⁴ For instance, the purpose of malware may range from collecting information, to testing a state's defenses, to launching a full scale attack. Furthermore, since remote penetrations are conducted by individuals, the purpose of the attack may be impossible to know without questioning the attacker.

⁴²⁵ Using active defenses in anticipatory self-defense will undoubtedly come under intense international scrutiny the first few times it happens and anger the host-state whose borders were electronically crossed. While states may legally act in anticipatory self-defense when it appears that an armed attack is imminent, it must be prepared to be questioned by other states who do not agree with its analysis. Ultimately the state's actions will be judged using the Rendulic Rule from a legal perspective and in the court of public opinion from a diplomatic perspective. Thus, anticipatory self-defense should only be used when a state feels that an after-the-fact analysis will truly support its actions. See *supra* note 366 and accompanying text.

⁴²⁶ See WILSON, *supra* note 15, at CRS-5 to CRS-7 (discussing the use of zombie computer systems to disguise the identity of an attacker); Ruth Wedgwood, *Proportionality, Cyberwar, and the Law of War*, in *COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW* 219, 227-30 (Michael N. Schmitt & Brian T. O'Donnell eds., Naval War College 2002) (discussing the use of looping and weaving to disguise the identity of an attacker). See generally Wheeler & Larsen, *supra* note 158 (discussing the technical methods of using intermediary computer systems to disguise the source of a cyberattack).

⁴²⁷ See generally Wheeler & Larsen, *supra* note 158 (discussing the technical capabilities of trace programs).

best of its technical capability and acts in good faith on the information on hand, it has met its international obligations.⁴²⁸ Second, states that refuse to comply with their international duty to prevent their territory from being used to commit cyberattacks have chosen to risk being held indirectly responsible by accident. After all, a state can avoid being the target of active defenses, even when attacks originate from it, by taking affirmative steps to prevent cyberattacks, such as enacting stringent criminal laws, enforcing those laws, and cooperating with victim-states to bring attackers to justice.

B. *Jus in Bello* Issues Related to the Use of Active Defenses

Decisions to use force, once in a state of armed conflict, are governed by *jus in bello*. States do not have a right to use unlimited force against other states during war.⁴²⁹ At its core, *jus in bello* uses four basic principles to regulate the conduct of states during warfare.⁴³⁰ These are the principles of distinction, necessity, humanity, and proportionality.⁴³¹

⁴²⁸ See *supra* note 366 and accompanying text.

⁴²⁹ This proposition is derived from Hague Convention IV, Annex, Article 22, which states, “[t]he right of belligerents to adopt means of injuring the enemy is not unlimited.” Hague Convention IV Respecting the Laws and Customs of War on Land and its Annex (Regulations), Oct. 18, 1907, 36 Stat. 2277, 1 Bevans 631 [hereinafter Hague IV].

⁴³⁰ COMMANDER’S HANDBOOK, *supra* note 59, §§ 5.3, 12.1.2.

⁴³¹ *Id.* Distinction, also referred to as discrimination, “is the requirement to distinguish combatants and military objectives from noncombatants . . . and civilian objects, and to attack only the former.” WINGFIELD, *supra* note 48, at 131. This principle is derived from Additional Protocol I, Article 48, which states, “[p]arties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.” Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I]. However, distinction does not protect civilians who directly participate in hostilities. *Id.*, art. 51(3).

Necessity limits the amount of force a state can use against legitimate targets “to that required for mission accomplishment and force protection,” and forbids using force purely “for the sake of destruction.” WINGFIELD, *supra* note 48, at 131.

Humanity prohibits the use of weapons designed to cause unnecessary suffering. WINGFIELD, *supra* note 48, at 131. This principle is derived from Hague Convention IV, Annex, Article 23, which states, “it is especially forbidden . . . to cause unnecessary suffering.” Hague IV, *supra* note 429.

Proportionality protects civilians and their property the same way necessity and humanity protect lawful targets from excessive uses of force. WINGFIELD, *supra* note 48, at 154. Understanding that attacks on legitimate targets will often cause incidental

1. Active Defenses, the Most Appropriate Forceful Response

While, as this article argues, states are legally authorized to respond to cyberattacks with force, states may only use force to the extent authorized under *jus in bello*.⁴³² In other words, unless limited by *jus in bello*, forcible responses are not limited to cyberspace. Therefore, it is worth explaining why state decision-makers should choose to use active defenses, as a matter of policy, as the most appropriate response to cyberattacks.

Active defenses are the most appropriate type of force to use against cyberattacks in light of the principles of *jus in bello*. First, in terms of military necessity, active defenses probably represent all the force needed to accomplish the mission of defending against a cyberattack. Active defenses can trace an attack back to its source and immediately disrupt it, whereas kinetic weapons will be slower and less effective than the lightning speed of a hack-back.⁴³³ Employing kinetic weapons over active defenses will not only be less effective, but will also violate the principle of necessity by employing force purely for destruction's sake. Second, in terms of proportionality, active defenses are less likely to cause disproportionate collateral damage than kinetic weapons. The traceback capabilities of active defenses allow them to target only the source of a cyberattack.⁴³⁴ While collateral damage may still result because the originating computer system may serve multiple functions, unless an attacker uses CNI to conduct the attack, damage should be fairly limited from the use of active defenses. Furthermore, since the majority of cyberattacks are conducted by non-state actors,⁴³⁵ it seems

damage beyond the lawful target itself, proportionality limits the use of force to situations in which the expected military advantage outweighs the expected collateral damage to civilians and their property. WINGFIELD, *supra* note 48, at 154–55. This principle is derived from Additional Protocol I, Article 51(5)(b), which states that it is prohibited to use force that “may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.” AP I, *supra* note 431.

⁴³² See *supra* note 171 and accompanying text.

⁴³³ See *supra* Part III.C (discussing defenses to cyberattacks).

⁴³⁴ See *id.* (discussing the capabilities of active defenses); Wheeler & Larsen, *supra* note 158, at 23–24 (discussing the use of automated tracer programs to find the originating point of a cyberattack). But see *infra* Part VII.A.3 (discussing the limitations of trace programs).

⁴³⁵ See Jensen, *supra* note 5, at 232.

unlikely that many attacks will come from CNI.⁴³⁶ Thus, active defenses provide states a way to surgically strike at their attacker with minimal risks of severe collateral damage to the host-state,⁴³⁷ thereby meeting the proportional requirement “to select [the] method or means of warfare likely to cause the least collateral damage and incidental injury, all other things being equal.”⁴³⁸ Finally, while not stemming from *jus in bello*, choosing active defenses versus kinetic weapons should reduce the chance of escalating these situations into full scale armed conflicts between states.

2. *Technological Limitations and Jus in Bello Analysis*

Unfortunately, despite the increased security that active defenses provide, using them is not without legal risk. Technological limitations may prevent states from conducting the surgical strikes envisioned with active defenses.⁴³⁹ The more an attacker routes his attack through intermediary systems, the more difficult it is to trace the attack.⁴⁴⁰

⁴³⁶ However, when cyberattacks originate from critical systems, the host-state bears responsibility for allowing them to be used in such a manner because states have an obligation to police their own citizens. *See supra* Part V.B. By failing to do so, states declare themselves sanctuary states and give other states the legal grounds to respond in self-defense to cyberattacks from them. *See supra* Part V.C–D. The principle of discrimination requires states to segregate their civilian objects from military objects. *See Jensen, supra* note 366, at 1174 (referencing AP I, Article 58). Thus, the host-state is effectively responsible for the collateral damage that occurs because it has allowed attackers within its territory to mix their means of attack with civilian objects making them dual use in nature and legitimate subjects of attack. *See Michael Schmitt, Wired Warfare: Computer Network Attack and the Jus in Bello, in COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW* 187, 198–99 (Michael N. Schmitt & Brian T. O’Donnell eds., Naval War College 2002).

⁴³⁷ *See Jensen, supra* note 366, at 1174 (noting that active defenses can be designed to simply shut a computer off to stop an attack, rather than permanently disabling it); Schmitt, *supra* note 436, at 204–05 (arguing that active defenses may simply shut down computer systems for a brief time, rather than having to use kinetic weapons, which, by their nature, cause physical destruction to achieve their objectives). *But see Wedgwood, supra* note 426, at 227–30 (arguing that it is harder to confine the effects of active defenses than it is with kinetic weapons because the links from a computer to the civilian infrastructure it controls are less apparent).

⁴³⁸ Schmitt, *supra* note 436, at 204.

⁴³⁹ *See Wedgwood, supra* note 426, at 227–30 (arguing that there is not enough time to properly map the functions of an attacking computer system when using active defenses, which may result in counter-strikes having broader than intended consequences).

⁴⁴⁰ *See generally Wheeler & Larsen, supra* note 158 (discussing ways to trace cyberattacks to their source).

Furthermore, complex traces take time, which is not always available during a moment of crisis.⁴⁴¹ Adding to these difficulties, trace programs often have problems pinpointing the source of an attack once an attacker terminates his electronic connection.⁴⁴² Sometimes these difficulties will simply result in a failure to identify the source of an attack; other times it may result in the incorrect identification of an intermediary system as the source of an attack.⁴⁴³ Even when the source of an attack is correctly identified, the victim-state's system administrator must map out the attacking computer system to distinguish its functions and the likely consequences that will result from shutting it down.⁴⁴⁴ However, system mapping takes time, often more time than a state has to make an informed decision.⁴⁴⁵ Sometimes an administrator will be able to map a system quickly, allowing states to make informed decisions about likely collateral damage. Other times a state will be forced to predict the likely consequences of using active defenses without having fully mapped a system. As a result, any state that employs active defenses runs the risk of accidentally targeting innocent systems and causing unintended, excessive collateral damage.⁴⁴⁶

To ensure the lawful use of active defenses in accordance with the principles of distinction and proportionality, states must do "everything feasible" to mitigate these risks.⁴⁴⁷ In the realm of active defenses, this

⁴⁴¹ See Wedgwood, *supra* note 426, at 227–30.

⁴⁴² See generally Wheeler & Larsen, *supra* note 158 (discussing ways to trace cyberattacks to their source).

⁴⁴³ See Wedgwood, *supra* note 426, at 227–30 (noting that looping and weaving techniques may cause faulty traces); WILSON, *supra* note 15, at 5–7 (noting that zombies are often used to conduct cyberattacks). See generally Wheeler & Larsen, *supra* note 158 (discussing ways to trace cyberattacks to their source).

⁴⁴⁴ See Barkham, *supra* note 29, at 82–83; Jensen, *supra* note 366, at 1184–85.

⁴⁴⁵ See Wedgwood, *supra* note 426, at 227–30.

⁴⁴⁶ See Barkham, *supra* note 29, at 82–83; Jensen, *supra* note 366, at 1178–79. Targeting innocent systems violates the principle of distinction, unless it meets the safe harbor of the Rendulic Rule. Jensen, *supra* note 366, at 1178–86. Causing excessive collateral damage in relation to the military advantage gained violates the principle of proportionality, unless it meets the safe harbor of the Rendulic Rule. *Id.*

⁴⁴⁷ Jensen, *supra* note 366, at 1183–86. This principle is derived from AP I, Article 57(2), which states:

- (a) those who plan or decide upon an attack shall:
 - (i) do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects . . . ;
 - (ii) take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event minimizing,

means doing everything feasible to identify (1) the computer system that launched the initial attack; and (2) the probable collateral damage that will result from using active defenses against that system.⁴⁴⁸ Once a state does everything feasible to ensure it has the right information and acts in good faith in accordance with *jus in bello*, it is legally protected from erroneous calculations, even when it targets civilian systems or causes excessive collateral damage in relation to its military objective.⁴⁴⁹ “The important point is that a [state] is required only to do what is feasible, given the prevailing circumstances, including the time [it] has to make a decision and the amount of information it has during that time.”⁴⁵⁰ Thus, states may still act with imperfect information, based on the way facts appear at the time, when the potential danger forces them to act.⁴⁵¹ The real test will be whether danger to the victim-state’s systems justified the use of active defenses in light of the likely collateral damage to the host-state.⁴⁵²

While beyond the scope of this article, states should consider several issues before they decide to implement active defenses. First, due to the compressed timelines of cyberattacks, a state may need to automate its active defenses so that it can respond in a timely manner. However, using automated defenses will increase the likelihood of violating the principles of distinction and proportionality. As a result, defenses should probably only be automated for detection purposes, requiring human analysis and approval before actually counter-striking. Second, just because it is legal to use active defenses under the circumstances described in this article, does not mean it is sound policy. States must

incidental loss of civilian life, injury to civilians and damage to civilian objects;

(iii) refrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.

AP I, *supra* note 431.

⁴⁴⁸ See Jensen, *supra* note 366, at 1183–86. Probable consequences are judged as the consequences that “may be ‘expected,’ not what is likely or possible, or even what is foreseeable.” *Id.* at 1179. See generally Brown, *supra* note 51, at 198–202 (discussing the requirements of distinction, necessity, humanity, and proportionality regarding cyberattacks).

⁴⁴⁹ See Jensen, *supra* note 366, at 1184–86 (discussing the legal protection granted to states and decision makers under the Rendulic Rule).

⁴⁵⁰ *Id.* at 1186.

⁴⁵¹ See *id.* at 1183.

⁴⁵² See Brown, *supra* note 51, at 201–02.

decide whether the diplomatic fallout is worth the risk. Unfortunately, technological limitations can cause state calculations to be erroneous at times, and cause civilian systems to be targeted or excessively damaged. States must decide that the second guessing that other states will engage in is worth the benefit gained from protecting their computer systems. Third, the servers from which the initial attacks originate may be intimately tied to important systems in the host-state, and if disrupted could have devastating effects and cause unnecessary suffering. This possibility must be factored into the state's evaluation of military necessity versus probable collateral damage, especially if a state responds with active defenses without fully mapping an attacking system. Fourth, states should carefully design their active defenses. Poorly coded active defense programs run the risk of self-propagating in cyberspace beyond their initial purpose, and can run the risk of evolving from a defensive program into a computer virus or worm whose damage goes far beyond its intended design. Since active defenses represent a new frontier in cyberwarfare, their initial use will be controversial, no matter the situation. States should expect public scrutiny and diplomatic protests until such time as active defenses are recognized as a lawful method of self-defense under international law.

VIII. Conclusion

Cyberattacks are one of the greatest threats to international peace and security in the twenty-first century. Securing cyberspace is an absolute imperative. In an ideal world, states would work together to eliminate the cyberthreat. Unfortunately, our world is no utopia, nor is it likely to become one. Sanctuary states refuse to cooperate with other states to eliminate cyberattacks, which casts doubt on reaching a global international agreement to secure cyberspace at any time in the near future. Perhaps one day global cooperation to eliminate cyberattacks will be a reality. Unless something changes to pressure sanctuary states into changing their behavior, there is no impetus for them to do so. As a result, states must use their imagination to get past the current legal roadblocks that prevent them from adequately addressing the current cyberthreat and compel sanctuary states into fulfilling their international duty to prevent cyberattacks.

The way to achieve this reality is to hold sanctuary states responsible for violating their duty to prevent cyberattacks and use active defenses against cyberattacks originating from within their borders. Not only will

this allow victim-states to protect themselves from cyberattacks, but it should also push sanctuary states into taking their international duty seriously. After all, no state wants another state using force within its borders, even electronically. Thus, the possibility that cyberattacks will be met with a forceful response is the hammer that can drive some sense into sanctuary states.

Since states do not currently use active defenses, any decision to use them will be a controversial change to state practice. This proposal is bound to be met with criticism on a number of fronts.⁴⁵³ However, there is sound legal authority to use active defenses against states that violate their duty to prevent cyberattacks. States that violate this duty, and refuse to change their practices, should be held responsible for all further attacks originating from within their borders in accordance with the law of war.⁴⁵⁴ At a time when cyberattacks threaten global security and states are scrambling to find ways to improve their cyberdefenses,⁴⁵⁵

⁴⁵³ The largest critiques are likely to come from those who believe that (1) cyberattacks are not acts of war and should be treated as a criminal matter or (2) victim-states should have to prove that a state initiated the cyberattack or exercised direct control over the attacker before it is allowed to use active defenses. However, some critics are even likely to critique this article's approach as not going far enough to protect state CNI from cyberattacks because it prevents states from using active defenses when attacks are not from sanctuary states. Critics who argue that cyberattacks cannot rise to the level of armed attacks miss the way the law has responded to unconventional attacks in the past. Furthermore, these critics also miss an important facet of international law—the theory and practice of reprisals, which can be used as an alternate basis to authorize active defenses against cyberattacks. *See supra* notes 350, 368 and accompanying text.

Critics who argue that this article goes too far by advocating for the use of active defenses without having to prove a state's involvement in the attacks miss the way that the law of state responsibility has evolved over the past thirty-years. Their arguments rest on the prevailing view of state responsibility for cyberattacks, which is rooted in outdated understandings of the law. *See supra* Part II.A (discussing the response crisis); *supra* Part V.C (analyzing the law of state responsibility); VI.B (analyzing state responsibility for cyberattacks).

Critics who argue that the approach advocated by this article does not go far enough to protect state CNI, and advocate using strict liability as the legal standard to protect CNI, miss a crucial part of the legal analysis—namely, just because CNI is under armed attack does not give a victim-state legal authority to violate the territorial integrity of the host-state. *See supra* notes 346, 352, 377 and accompanying text.

⁴⁵⁴ Today, state responsibility for the actions of non-state actors results from a state's failure to live up to their international duties to other states with respect to those non-state actors. *See supra* Part V.C. This includes the duty to prevent cyberattacks. *See supra* Part VI.B–D.

⁴⁵⁵ During President George W. Bush's administration, the United States initiated a \$30 billion cyberdefense plan to protect government computer networks from attack. Since President Obama has taken office, he has identified cybersecurity as one of the most

there is no reason to shield sanctuary states from the lawful use of active defenses by victim-states and every reason to enhance state defenses to cyberattacks by using them.

important national security concerns of the United States and has ordered a review of U.S. cyberdefenses to find ways to improve cybersecurity. The review of U.S. cyberdefenses is still ongoing at the time of this article's submission. However, one report already prepared for the President recommends a reexamination of the law regarding military responses to cyberattacks. See Keith Epstein, *U.S. is Losing Global Cyberwar, Commission Says*, BUSINESSWEEK.COM, Dec. 7, 2008, http://www.businessweek.com/bwdaily/dnflash/content/dec2008/db2008127_817606.htm; Peter Eisler, *Raids on Federal Computer Data Soar; "Major Intrusions" on Networks are Up 40%*, USA TODAY, Feb. 17, 2009, at 1A; Byron Acohido, *Obama Taps Cybersecurity Expert to Assess U.S. Defenses*, USA TODAY, Feb. 17, 2009, at 8B; Byron Acohido, *White House Urged to Stop Cyberattacks*, USA TODAY.COM, Mar. 11, 2009, <http://blogs.usatoday.com/technologylive/2009/03/the-united-stat.html>; CTR. FOR STRATEGIC AND INT'L STUD., COMM'N ON SECURING CYBERSPACE FOR THE 44TH PRESIDENCY, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY 8 (2008) (recommending to the President to direct the Attorney General to reexamine the law and "issue guidelines as to the circumstances and requirements for the use of . . . [the] military . . . in cyber incidents").

HALLIBURTON HEARS A WHO? POLITICAL QUESTION
DOCTRINE DEVELOPMENTS IN THE GLOBAL WAR ON
TERROR AND THEIR IMPACT ON GOVERNMENT
CONTINGENCY CONTRACTING

MAJOR CHAD C. CARTER*

*So you know what I think? Why, I think that there must
Be someone on top of that small speck of dust!
Some sort of a creature of very small size,
too small to be seen by an elephant's eyes*¹

. . . .

*"I think you're a fool!" laughed the sour kangaroo
And the young kangaroo in her pouch said, "Me, too!
You're the biggest blame fool in the Jungle of Nool!"*²

. . . .

*"For almost two days you've run wild and insisted
On chatting with persons who've never existed.
Such carryings-on in our peaceable jungle!*

* Judge Advocate, U.S. Air Force. Presently assigned as program counsel in the Contract Law Division of the Air Force Materiel Command Law Office, Wright-Patterson Air Force Base, Dayton, Ohio. LL.M., 2009, The Judge Advocate Gen.'s Legal Ctr. & Sch., Charlottesville, Va.; J.D., 1997, Southern University Law Center; B.A., 1993, Texas Christian University. Previous assignments include Deputy Staff Judge Advocate, 2d Bomb Wing, Barksdale Air Force Base, La., 2007–2008; Chief of Adverse Actions, Headquarters, 8th Air Force, Barksdale Air Force Base, La., 2006–2007; Assistant Professor of Law, U.S. Air Force Academy, Colo., 2004–2006; Associate Counsel, Defense Contract Management Agency (DCMA), Dallas, Tex., 2002–2004; Area Defense Counsel, Altus Air Force Base, Okla., 2000–2002; Assistant Staff Judge Advocate, 97th Air Mobility Wing, Altus Air Force Base, Okla., 1999–2000. Member of the bars of Texas and Louisiana. This article was submitted in partial completion of the Master of Laws requirements of the 57th Judge Advocate Officer Graduate Course. The views expressed in this article are those of the author and interviewees and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

¹ DR. SEUSS, HORTON HEARS A WHO! 5 (1954). In this children's book, a speck of dust on a clover, which is in fact a tiny planet inhabited by creatures known as Whos, speaks to the main character, an elephant named Horton. *Id.* For the majority of the story, Horton is the only character who can hear the Whos and he is ridiculed by the other residents of the Jungle of Nool because of his belief in the Whos' existence. *Id.*

² *Id.* at 14.

*We've had quite enough of your bellowing bungle!*³

— *Horton Hears a Who!*

I. Introduction

Recent court decisions exhibit the potential for increased defense contractor⁴ liability,⁵ which could, in turn, increase the costs of Government contingency contracting⁶ in the Global War on Terror

³ *Id.* at 36.

⁴ A defense contractor is “[a]ny individual, firm, corporation, partnership, association, or other legal non-Federal entity that enters into a contract directly with the Department of Defense to furnish services, supplies, or construction.” U.S. DEP’T OF DEFENSE, INSTR. 3020.41, CONTRACTOR PERSONNEL AUTHORIZED TO ACCOMPANY THE U.S. ARMED FORCES para. E2.1.5 (3 Oct. 2005).

⁵ See 22 NASH & CIBINIC REP. ¶ 44 (2008) [hereinafter NASH & CIBINIC REP.] (discussing *Lane v. Halliburton*, 529 F.3d 548 (5th Cir. 2008)).

The U.S. Court of Appeals for the Fifth Circuit has opened the door to lawsuits by or on behalf of contractor employees who are injured or killed while working in combat zones The Fifth Circuit concluded that the tort claims could be litigated without delving into political questions.

. . . .

In allowing this case to go to trial, the Fifth Circuit has more widely opened the door for suits by contractor employees who work in combat zones. This obviously imposes significant risks on such contractors and may affect the ability of the Government to persuade such contractors to undertake this type of work.

Id.; see also *infra* Section V.

⁶ See *infra* Section VIII. Regarding the term contingency contracting, Defense Acquisition University states “[a]t this time there is not universal agreement as to a definition of this term[.]” but defines the term for academic purposes as “[d]irect contracting support to tactical and operational forces engaged in the full spectrum of armed conflict and Military Operations Other Than War, both domestic and overseas.” Defense Acquisition University, CON 234 Contingency Contracting, Pre-Course Materials, available at: <http://www.dau.mil/registrar/pre-courses/CON%20234%20Pre-Course%20Materials.pdf> (last visited July 9, 2009). The definition is “purposely exclusive of: military training exercises, routine installation and base operations, and systems/inventory control point contracting,” both inside and outside the continental United States. *Id.* The major difference between these types of contracting and contingency contracting is “the element of *immediate risk* to human life or significant

(GWOT).⁷ Specifically, the Fifth and Eleventh Federal Circuit Courts of Appeals have allowed tort cases⁸ by military members and U.S. civilians injured in Iraq and Afghanistan to proceed.⁹ Significantly, such cases may involve “political questions” that the Judicial Branch is ill-equipped to decide.¹⁰ Some defense contractor advocates claim these actions must be dismissed, else there be grim consequences for Government contingency contracting.¹¹ Much like Horton’s singular awareness of the

national interests.” *Id.* This is the context in which this article uses the term government contingency contracting.

⁷ See generally Jeffrey F. Addicott, *The Political Question Doctrine and Civil Liability for Contracting Companies on the “Battlefield,”* 28 REV. LITIG. 343, 343 n.2 (2008) (“The term ‘War on Terror’ is used both as a metaphor to describe a general conflict against all international terrorist groups and, more precisely, to describe the ongoing international armed conflict between the United States of America and the ‘Taliban, al-Qaeda, or associated forces.’”) (citing 10 U.S.C. § 948a(1)(i) (2006)). Recent news reports indicate a desire by the Obama Administration to replace the GWOT label with the term “overseas contingency operations.” See generally Jon Ward, *White House: ‘War on Terrorism’ is Over*, WASHINGTONTIMES.COM, Aug. 6, 2009, http://www.washingtontimes.com/news/2009/aug/06/white-house-war-terrorism-over/?feat=home_headlines; Scott Wilson & Al Kamen, *‘Global War On Terror’ Is Given New Name*, WASHINGTONPOST.COM, Mar. 25, 2009, <http://www.washingtonpost.com/wp-dyn/content/article/2009/03/24/AR2009032402818.html>. Because the GWOT label was the appropriate terminology at the time of the events in the relevant cases discussed in this article, this article continues to use that term.

⁸ See generally LAWRENCE J. MCQUILLAN & HOVANNES ABRAMYAN, U.S. TORT LIABILITY INDEX: 2008 REPORT 7 (2008).

A tort, French for “wrong,” is best defined as wrongful conduct by one individual that results in injury to another. A tort has been committed when someone has suffered injury caused by the failure of another person to exercise a required duty of care. The actor is to blame, and the injured party is entitled to recover damages. The function of torts is to provide the injured party with a remedy, not to punish the actor.

Id.

⁹ See *Lane*, 529 F.3d 548; *McMahon v. Presidential Airways, Inc.*, 502 F.3d 1331 (11th Cir. 2007).

¹⁰ See *infra* Section II.

¹¹ See generally Brief for Prof’l Servs. Council as Amicus Curiae Supporting Defendant, *Smith-Idol v. Halliburton*, 2006 U.S. Dist. LEXIS 75574, (S.D. Tex. 2006) (No. H-06-1168).

[T]he devastating effects of such state-law tort suits would be far more profound than financial. If federal courts [allow such suits to proceed,] existing and future battlefield contractors, out of fear of state-law liability, may decline to follow, or unilaterally alter or deviate from, the military’s combat zone instructions

Whos, are defense contractors by themselves aware of an impending crisis in Government contingency contracting? Does this “tiny planet” of a presaged broken combat zone procurement system really exist?

Using established political question doctrine precedent, federal courts recently designed a workable analytical framework for the identification of political questions in a modern contingency environment. These decisions protect military policy and decision-making from improper judicial intervention. This development is important because of its potential effect on Government contingency contracting.

Before the court cases are examined, it is important to review what the political question doctrine is, why it is important, and how it has developed over time. Sections II, III, and IV of this article examine the relevance and history of the political question doctrine. The doctrine’s impact on the federal judiciary’s involvement in foreign and military affairs is also addressed. Sections V and VI of this article discuss recent GWOT cases involving the doctrine and its current status involving tort suits against defense contractors in contingency environments. Finally, Sections VII and VIII of this article clarify the impact of these developments on Government contingency contracting.

The recent developments in political question doctrine case law are significant to the future of Government contingency contracting. However, they are not catastrophic—although portrayed as such by some defense contractor advocates.¹² There will not be an explosion of contracting costs passed on to the Government. There will not be a mass refusal of defense contractors to accept contingency contracts. There will not be chaos on the battlefield. Such predictions are nothing more than “bellowing bungle,” and this article demonstrates why.

II. The Political Question Doctrine: What Is It? Why Is It Important?

Before the impact of the cases on Government contingency contracting can be accurately analyzed, it is first necessary to establish

Id.

¹² See, e.g., *supra* note 11.

the meaning of the term political question doctrine and explain its relevance to contemporary legal analysis.

What is the political question doctrine? According to Chief Justice John Marshall, “[q]uestions, in their nature political, or which are, by the constitution and laws, submitted to the executive, can never be made in [the U.S. Supreme Court].”¹³ In 2004, the Court held “[s]ometimes . . . the law is that the judicial department has no business entertaining [a] claim of unlawfulness—because the question is entrusted to one of the political branches or involves no judicially enforceable rights. Such questions are said to be ‘nonjusticiable,’ or ‘political questions.’”¹⁴ While judicial abstention of political questions has remained a consistent practice throughout the history of American jurisprudence,¹⁵ what actually makes up a political question is less obvious.¹⁶

A portion of the confusion surrounding the doctrine¹⁷ originates from its label. Some scholars contend the term “political” should more appropriately be interpreted as “discretionary.”¹⁸ Furthermore, just

¹³ *Marbury v. Madison*, 5 U.S. (1 Cranch) 137, 170 (1803).

¹⁴ *Vieth v. Jubelirer*, 541 U.S. 267, 277 (2004) (citations omitted).

¹⁵ See, e.g., *supra* notes 13–14 and accompanying text.

¹⁶ See LOUIS HENKIN, *FOREIGN AFFAIRS AND THE CONSTITUTION* 144 (1996) (“That there is a ‘political question’ doctrine is not disputed, but there is little agreement as to anything else about it—its constitutional basis and scope; whether abstention is required or optional; how the courts decide whether a question is ‘political,’ and which questions are.” (end note omitted)); see also *Lane v. Halliburton*, 529 F.3d 548, 559 (5th Cir. 2008) (“[W]hether an issue presents a nonjusticiable political question cannot be determined by a precise formula.”) (quoting *Saldano v. O’Connell*, 322 F.3d 365, 368 (5th Cir. 2003)); *Comm. of U.S. Citizens Living in Nicar. v. Reagan*, 859 F.2d 929, 933 (D.C. Cir. 1988) (“No branch of the law of justiciability is in such disarray as the doctrine of the ‘political question.’”) (quoting CHARLES ALAN WRIGHT, *THE LAW OF FEDERAL COURTS* 74 (4th ed. 1983)); *Ibrahim v. Titan Corp.*, 391 F. Supp. 2d 10, 15 (D.D.C. 2005) (contending the political question doctrine “may lack clarity”); NORMAN REDLICH ET AL., *CONSTITUTIONAL LAW* 51 (5th ed. 2008) (“[T]hough Chief Justice Marshall stated that political questions were not within judicial competence, he did not indicate what made a question political within the meaning of the rule.”); Maurice Finkelstein, *Judicial Self-Limitation*, 37 HARV. L. REV. 338, 344 (1924) (“[T]he chaos that exists in the cases with reference to what are and what are not political questions defies classification.”); A.E. Gold, *Jurisdiction and the Supreme Court Over Political Questions: What is a Political Question?*, 9 CORNELL L.Q. 50, 50 (1923) (“[T]he line of demarcation between justiciable and political questions has never been clearly drawn.”).

¹⁷ See generally *supra* note 16.

¹⁸ Edwin B. Firmage, *The War Powers and the Political Question Doctrine*, 49 U. COLO. L. REV. 65, 68–69 (1977) (“Chief Justice Marshall used the term ‘political’ to mean ‘discretionary’ . . . [W]hen a discretionary function of the President or Congress is

because an issue can be termed political in nature does not mean the political question doctrine will automatically bar federal courts from deciding it.¹⁹ In attempting to identify political questions it is more important to use as a guide those issues historically viewed as “outside the sphere of judicial power”²⁰ than it is to look for a magical source of direction in the term political.

The political question doctrine relates directly to the U.S. Government’s separation of powers.²¹ The doctrine “excludes from judicial review those controversies which revolve around policy choices and value determinations constitutionally committed for resolution to the halls of Congress or the confines of the Executive Branch.”²² Furthermore, “[b]ecause political questions are nonjusticiable under Article III of the Constitution, courts lack jurisdiction to decide such cases.”²³ The doctrine serves to “prevent[] federal courts from overstepping their constitutionally defined role.”²⁴ Correspondingly, the political question doctrine performs an important function in protecting the separation of powers.

sought to be adjudicated, the Court will, in most cases, refuse independent review because the nature of the issue is political and not juridical.”)

¹⁹ *Japan Whaling Ass’n v. Am. Cetacean Soc’y*, 478 U.S. 221, 229 (1986) (“[N]ot every matter touching on politics is a political question.”); *INS v. Chadha*, 462 U.S. 919, 942–43 (1983) (“[T]he presence of constitutional issues with significant political overtones does not automatically invoke the political question doctrine. Resolution of litigation challenging the constitutional authority of one of the three branches cannot be evaded by courts because the issues have political implications in the sense urged by Congress.”); *Suhail Najim Abdullah Al Shimari v. CACI Premier Tech., Inc.*, 2009 U.S. Dist. LEXIS 29995, at *13 (E.D. Va. 2009) (“The concern is not with ‘political cases’ carrying the potential to stir up controversy, but instead with ‘political questions’ which, by their nature, create separation of powers concerns.”) (citing *Baker v. Carr*, 369 U.S. 186, 217 (1962)).

²⁰ LOUIS FISHER, *AMERICAN CONSTITUTIONAL LAW* 103 (6th ed. 2005) (quoting *Velvel v. Johnson*, 287 F. Supp. 846, 850 (D. Kans. 1968)).

²¹ *Lane*, 529 F.3d at 559 (“[T]he purpose of the political question doctrine is to bar claims that have the potential to undermine the separation-of-powers design of our federal government.”).

²² *Lessin v. Kellogg Brown & Root*, 2006 U.S. Dist. LEXIS 39403, at *3 (S.D. Tex. 2006) (quoting *Japan Whaling Ass’n*, 478 U.S. at 230).

²³ *Id.* (citing *Occidental of UMM al Qaywayn, Inc. v. A Certain Cargo of Petroleum*, 577 F.2d 1196, 1203 (5th Cir. 1978)).

²⁴ *McMahon v. Presidential Airways, Inc.*, 502 F.3d 1331, 1357 (11th Cir. 2007), (citing *Baker*, 369 U.S. at 210).

Like the other self-imposed limits on judicial review (e.g., standing, ripeness, mootness, etc.), the political question doctrine is not expressly mentioned in the Constitution.²⁵ However, while other limits on judicial review focus on the status of the party bringing the action,²⁶ the political question doctrine instead focuses on the substance of the issue presented.²⁷ In that sense, the doctrine functions as a merit determination of the issue at hand. Consequently, some scholars argue the doctrine should be viewed differently than the other limitations on judicial review.²⁸

²⁵ See Firmage, *supra* note 18, at 66 (“Unchecked judicial review is avoided in part by constraints imposed by the judicial branch itself.”); see also Gold, *supra* note 16, at 53 (“The refusal of the Supreme Court to take jurisdiction of ‘political questions’ . . . constitutes an entirely self-imposed limitation. There is no provision of the Constitution which requires it.”).

²⁶ Linda Champlin & Alan Schwarz, *Political Question Doctrine and Allocation of the Foreign Affairs Power*, 13 HOFSTRA L. REV. 215, 231–32 (1985).

²⁷ *Made in USA Found. v. United States*, 56 F. Supp. 2d 1226, 1254 (N.D. Ala. 1999).

An important consequence of the political question doctrine is that a holding of its applicability to a theory of a cause of action renders the government conduct immune from judicial review. Unlike other restrictions on judicial review—doctrines such as case or controversy requirements, standing, ripeness, and prematurity, abstractness, mootness, and abstention—all of which can be cured by different factual circumstances, a holding of nonjusticiability is absolute in its foreclosure of judicial scrutiny.

Id. (citing RONALD D. ROTUNDA & JOHN E. NOWAK, 1 TREATISE ON CONSTITUTIONAL LAW § 2.16 (2d ed. 1992)); Champlin & Schwarz, *supra* note 26, at 231–32; Fritz W. Scharpf, *Judicial Review and the Political Question: A Functional Analysis*, 75 YALE L. J. 517, 537–38 (1966).

²⁸ See Champlin & Schwarz, *supra* note 26, at 231–32.

Nonjusticiability . . . exists separately from the political question doctrine. Standing, ripeness and mootness, for example, are situations where the status of a party disables her from invoking judicial action over an issue. In the political question context, by contrast, the issue itself, independent of the status of the parties, has been termed non-justiciable.

Id. Furthermore, there is a lack of consensus of nomenclature as to how the term political question doctrine relates to the term nonjusticiable. *Cf.*, *supra* note 27; *Nejad v. United States*, 724 F. Supp. 753, 755 (C.D. Cal. 1989) (equating the terms political and nonjusticiable.); ROTUNDA & NOWAK, *supra* note 27, § 2.16(a) (contending the doctrine “should more properly be called the doctrine of nonjusticiability, that is, a holding that the subject matter is inappropriate for judicial consideration”).

The political question doctrine generates strong opinions among legal scholars. Because the doctrine involves a court's refusal to exercise jurisdiction in matters where it otherwise would,²⁹ some scholars criticize the doctrine³⁰ while others laud it.³¹ Critics view it as a form of "judicial avoidance" whereby federal courts improperly abandon their responsibility to interpret the Constitution.³² Other critics go so far as to declare the doctrine an affront to the Constitution and its history.³³ These

²⁹ Potts v. Dyncorp Int'l, LLC, 465 F. Supp. 2d 1245, 1248 (M.D. Ala. 2006) ("If the doctrine applies, courts refuse to exercise jurisdiction they otherwise might have.")

³⁰ See, e.g., ALEXANDER M. BICKEL, *THE LEAST DANGEROUS BRANCH* 184 (2d ed. 1986). The political question doctrine is founded on

the Court's sense of lack of capacity, compounded in unequal parts of (a) the strangeness of the issue and its intractability to principled resolution; (b) the sheer momentousness of it, which tends to unbalance judicial judgment; (c) the anxiety, not so much that the judicial judgment will be ignored, as that perhaps it should but will not be; (d) finally ("in a mature democracy"), the inner vulnerability, the self doubt of an institution which is electorally irresponsible and has no earth to draw strength from.

Id.; THOMAS M. FRANCK, *POLITICAL QUESTIONS/JUDICIAL ANSWERS: DOES THE RULE OF LAW APPLY TO FOREIGN AFFAIRS?* 4 (1992) ("[T]he abdicationist tendency, primarily expounded in what has become known as the 'political question doctrine,' is not only not required by but wholly incompatible with American constitutional theory."); Firmage, *supra* note 18, at 66.

The importance and seriousness of the debate arise primarily from one fact. Under the political question doctrine, a court may refuse to render an independent ruling on an issue arising under the Constitution in a case in which all normal prerequisites, constitutional and non-constitutional, to an independent juridical determination have been met.

Id.; *infra* notes 32–35.

³¹ See, e.g., *infra* note 36.

³² Scharpf, *supra* note 27, at 535–38 ("[W]hen it holds that a question is 'political' rather than 'judicial,' the Court renounces [its] responsibility altogether, and leaves the performance of this function to the political institutions. . . . When it applies the doctrine to a question, the Court abdicates its responsibility 'to say what the law is.'"); Champlin & Schwarz, *supra* note 26, at 220 (contending invocation of the political question doctrine is an "extreme position" where a court "abdicate[s] its most important function—Constitutional review").

³³ Jonathan R. Siegel, *Political Questions and Political Remedies*, in *THE POLITICAL QUESTION DOCTRINE AND THE SUPREME COURT OF THE UNITED STATES* 243, 243 (Nada Mourtada-Sabbah & Bruce E. Cain eds., 2007).

individuals contend the courts are better suited than the electoral process at protecting and interpreting the Constitution.³⁴ Such scholars prefer courts which operate on a system of well-reasoned decisions and precedent to political branches that operate merely on “majoritarian preference.”³⁵ Conversely, other scholars view the doctrine as an important element of good Government.³⁶ Not only has the very existence of the political question doctrine served as a lightning rod for scholarly debate, but disagreement also exists among scholars as to the procedural implication of the doctrine.

Ultimately, courts have decided the political question doctrine can be implicated in one of two ways—on textual or prudential grounds.³⁷ Textual implication arises when the Constitution specifically grants the power to decide a particular matter to one or both of the political

The puzzling and troubling feature of the political question doctrine is the potential it seems to have to render constitutional provisions meaningless. After armed struggle and tremendous political effort, our ancestors gave us the magnificent achievement of a written Constitution that limits the powers of government. Under the political question doctrine, however, the principal enforcement mechanism for those constitutional limits—judicial review—is not available for certain constitutional provisions.

Id. (footnote omitted).

³⁴ *Id.* at 244.

[T]he electoral process lacks crucial structural elements provided by the judicial process that make the latter a proper mechanism for the enforcement of constitutional constraints. The judicial process is mandatory in nature; it focuses on particular issues; it provides a statement of reasons for its decisions; it operates within a system of precedent; and it operates according to law, not according to majoritarian preference. These features of the judicial process . . . are not found in the electoral process and are crucial to the appropriateness of the judicial process for resolving constitutional issues.

Id.

³⁵ *Id.*

³⁶ See Finkelstein, *supra* note 16, at 345 (contending the doctrine supports the public’s interest in “effective legal action”).

³⁷ See generally Rachel E. Barkow, *The Rise and Fall of the Political Question Doctrine*, in *THE POLITICAL QUESTION DOCTRINE AND THE SUPREME COURT OF THE UNITED STATES*, *supra* note 33, at 23; Joseph H.L. Perez-Montes, Comment, *Is the Political Question Doctrine a Viable Bar to Tort Claims Against Private Military Contractors?*, 83 *TUL. L. REV.* 219, 228–30 (2008).

branches.³⁸ More controversially, prudential implication arises when courts look outside the text of the Constitution to determine whether a particular matter *should* be decided by the judicial branch.³⁹ The tension between these two competing versions of political question doctrine philosophy has generated scholarly debate.⁴⁰

Beyond the political question doctrine's meaning and relevance, an appreciation of the doctrine's impact on today's cases requires an understanding of the doctrine's historical basis and development.

III. History and Development of the Political Question Doctrine

Although the doctrine's current analytical framework originates from a handful of landmark U.S. Supreme Court opinions,⁴¹ the political question doctrine arrived in America as a component of the common law.⁴² Some scholars argue Alexander Hamilton contemplated the basic principle behind the doctrine in *The Federalist Papers*.⁴³ However, John Marshall deserves much of the credit for bringing the doctrine to the forefront of American jurisprudence.⁴⁴ Three years before Marshall discussed political questions as a limit on judicial review in *Marbury v. Madison*,⁴⁵ he warned of the potential danger of a court without jurisdictional limits.⁴⁶ Marshall cautioned that "if the judicial power extended to every question under the constitution, it would involve almost every subject proper for legislative discussion and decision."⁴⁷ This would undermine the separation of powers and "the other

³⁸ See generally Barkow, *supra* note 37; Perez-Montes, *supra* note 37, at 228–30.

³⁹ See generally Barkow, *supra* note 37; Perez-Montes, *supra* note 37, at 228–30.

⁴⁰ See generally Perez-Montes, *supra* note 37, at 228–30 (providing a brief summary of the debate between Professor Herbert Wechsler and Professor Alexander Bickel on this subject).

⁴¹ E.g., *Baker v. Carr*, 369 U.S. 186 (1963); *Marbury v. Madison*, 5 U.S. (1 Cranch) 137 (1803).

⁴² Firmage, *supra* note 18, at 68.

⁴³ Barkow, *supra* note 37, at 24 (claiming "Hamilton . . . recognized a constitutionally based political question doctrine . . ." in *The Federalist No. 78*). See THE FEDERALIST NO. 78 (Alexander Hamilton).

⁴⁴ See generally *infra* notes 45–51 and accompanying text.

⁴⁵ 5 U.S. (1 Cranch) 137 (1803).

⁴⁶ Barkow, *supra* note 37, at 25.

⁴⁷ *Id.* (quoting Representative John Marshall, Speech on the Floor of the House of Representatives (Mar. 7, 1800), in 18 U.S. (5 Wheat.) app. note I, at 16–17 (1820)).

departments would be swallowed up by the judiciary.”⁴⁸ Marshall carried these notions of judicial restraint with him to the Supreme Court.

Marbury v. Madison is of course the case in which judicial review was “firmly established as a keystone of our constitutional jurisprudence.”⁴⁹ However, *Marbury* also conveyed the message that judicial review is not without limitation: “the President is invested with certain important political powers, in the exercise of which he is to use his own discretion, and is accountable only to his country in his political character, and to his own conscience.”⁵⁰ Those words set forth the principle that some discretionary actions of the political branches cannot be reviewed by the courts.⁵¹ Therefore, despite not being widely known as such, *Marbury* was quite significant in the development of the political question doctrine.

The most consequential U.S. Supreme Court case regarding the political question doctrine is a voting rights reapportionment case from 1963, *Baker v. Carr*.⁵² In *Baker*, the Court held that the determination of whether a matter has been committed to another branch of the Federal Government “is itself a delicate exercise in constitutional interpretation, and is a responsibility of this Court as ultimate interpreter of the Constitution.”⁵³ The *Baker* case delineated six criteria⁵⁴ to be used in determining the existence of a political question:

[1] a textually demonstrable constitutional commitment of the issue to a coordinate political

⁴⁸ *Id.*

⁴⁹ Louis Henkin, *Is There a “Political Question Doctrine?”* 85 YALE L.J. 597, 600 (1976).

⁵⁰ *Marbury*, 5 U.S. at 165–66.

⁵¹ Nada Mourtada-Sabbah & John W. Fox, *Two Centuries of Changing Political Questions in Cultural Context*, in THE POLITICAL QUESTION DOCTRINE, *supra* note 33, at 90.

⁵² 369 U.S. 186 (1963); see *Rogers v. Lodge*, 458 U.S. 613, 634 (1982) (contending *Baker* “represents one of the great landmarks in the history of [the U.S. Supreme Court’s] jurisprudence”); *Developments in the Law: Access to Courts*, 122 HARV. L. REV. 1151, 1195 (2009) [hereinafter *Developments*] (describing *Baker* as the case which “announced [the political question] doctrine’s modern contours”).

⁵³ *Baker*, 369 U.S. at 211.

⁵⁴ The *Baker* criteria are also described as formulations, tests, and indicia. See *id.* at 217 (describing the criteria as formulations); *Vieth v. Jubelirer*, 541 U.S. 267, 277 (2004) (describing the criteria as tests); *McMahon v. Presidential Airways, Inc.*, 502 F.3d 1331, 1357 (11th Cir. 2007) (describing the criteria as indicia). However, the *Baker* criteria are not factors to be weighed against one another. See generally *Baker*, 369 U.S. at 218–24.

department; or [2] a lack of judicially discoverable and manageable standards for resolving it; or [3] the impossibility of deciding without an initial policy determination of a kind clearly for non-judicial discretion; or [4] the impossibility of a court's undertaking independent resolution without expressing lack of respect due coordinate branches of government; or [5] an unusual need for unquestioning adherence to a political decision already made; or [6] the potentiality of embarrassment from multifarious pronouncements by various departments on one question.⁵⁵

These six *Baker* criteria serve as standards with which political question cases are to be measured.⁵⁶ Unless one of the six presents itself in a particular case, there should be no dismissal on political question grounds.⁵⁷

Subsequent cases further clarified and refined the *Baker* criteria.⁵⁸ For example, somewhat recently the Court held the *Baker* criteria “are probably listed in descending order of both importance and certainty.”⁵⁹ Other cases suggested the six criteria could be viewed together or combined into more succinct inquiries.⁶⁰ Despite these suggestions,

⁵⁵ *Baker*, 369 U.S. at 217.

⁵⁶ *Ibrahim v. Titan Corp.*, 391 F. Supp. 2d 10, 15 (D.D.C. 2005) (“The political question doctrine may lack clarity, but it is not without standards.”) (citing *Comm. of U.S. Citizens Living in Nicar. v. Reagan*, 859 F.2d 929, 933 (D.C. Cir. 1988)).

⁵⁷ *Baker*, 369 U.S. at 217 (“Unless one of these formulations is inextricable from the case at bar, there should be no dismissal for nonjusticiability on the ground of a political question’s presence.”); see *Occidental of Umm al Qaywayn, Inc. v. A Certain Cargo of Petroleum*, 577 F.2d 1196, 1203 (5th Cir. 1978) (“[T]he inextricable presence of one or more of these factors will render the case nonjusticiable under the Article III ‘case or controversy’ requirement . . .”).

⁵⁸ See *infra* notes 59–60.

⁵⁹ *Vieth*, 541 U.S. at 278.

⁶⁰ See *Goldwater v. Carter*, 444 U.S. 996 (1979). In a concurring opinion, Justice Powell contended a court’s analysis of political question doctrine issues “incorporates three inquiries: (i) Does the issue involve resolution of questions committed by the text of the Constitution to a coordinate branch of government? (ii) Would resolution of the question demand that a court move beyond areas of judicial expertise? (iii) Do prudential considerations counsel against judicial intervention?” *Id.* at 998; see also *Nixon v. United States*, 506 U.S. 224 (1993).

[T]he concept of a textual commitment to a coordinate political department is not completely separate from the concept of a lack of judicially discoverable and manageable standards for resolving it; the

today's cases still prominently use the *Baker* criteria to identify political questions.⁶¹ These criteria form the primary analytical framework relied upon by courts today to decide GWOT political question cases.⁶²

IV. The Political Question Doctrine in Relation to Foreign Affairs and the Military

Despite the long history of judicial involvement in American foreign affairs,⁶³ courts today are somewhat reluctant to inject themselves into matters involving foreign affairs or the U.S. military.⁶⁴ This reluctance comes from the perception that the political branches are better equipped to handle such affairs.⁶⁵

lack of judicially manageable standards may strengthen the conclusion that there is a textually demonstrable commitment to a coordinate branch.

Id. at 228–29.

⁶¹ *Lane v. Halliburton*, 529 F.3d 548, 558 (5th Cir. 2008); *McMahon v. Presidential Airways, Inc.*, 502 F.3d 1331, 1358 (11th Cir. 2007) (“A case may be dismissed on political question grounds if—and only if—the case will require the court to decide a question possessing one of these six characteristics.”); *Developments, supra* note 52, at 1195 (“In its foreign relations jurisprudence following [*Baker*], the Supreme Court has clarified these categories but never increased their number.”) (citing as examples *Japan Whaling Ass’n v. Am. Cetacean Soc’y*, 478 U.S. 221, 230 (1986); *Vieth*, 541 U.S. at 277–78).

⁶² See *infra* Sections V and VI.

⁶³ See generally LOUIS FISHER & NADA MOURTADA-SABBAH, *IS WAR A POLITICAL QUESTION?* (2001) (containing detailed discussion of numerous such cases from 1789–1999).

Contrary to the general impression that war power disputes present political questions beyond the scope of judicial scrutiny, courts have often regarded the exercise of war powers by the political departments as subject to their independent judicial review. Throughout the past two centuries, federal courts . . . have reviewed a broad range of issues involving foreign conflicts . . .

Id. at 81.

⁶⁴ See generally *Baker v. Carr*, 369 U.S. 186 (1963); *infra* notes 68–74 and accompanying text.

⁶⁵ *Baker*, 369 U.S. at 211 (“Not only does resolution of such issues frequently turn on standards that defy judicial application, or involve the exercise of a discretion demonstrably committed to the executive or legislature; but many such questions uniquely demand single-voiced statement of the Government’s views.”).

The first half of the twentieth century marshaled a judicial philosophy that clearly favored use of the doctrine in foreign affairs cases. In “sweeping judicial dicta,” several Supreme Court cases indicated “all questions touching foreign relations are political questions.”⁶⁶

More recently, courts have continued to defer to the political branches in matters of foreign policy and military affairs.⁶⁷ Our system of separation of powers affords great deference to the “underlying factual or legal determinations” made by the President in his conduct of foreign relations.⁶⁸ Policy decisions regarding the employment of U.S. military forces in combat belong to the political branches, not the courts⁶⁹ The Supreme Court has held that, due to their “complex, subtle, and professional” nature, decisions as to the “composition, training, equipping, and control of a military force” are “subject *always*” to the

⁶⁶ Thomas M. Franck & Clifford A. Bob, *The Return of Humpty-Dumpty: Foreign Relations Law After the Chadha Case*, 79 AM. J. INT’L L. 912, 953 (1985) (citing as examples *Oetjen v. Cent. Leather Co.*, 246 U.S. 297 (1918); *Chicago & S. Airlines, Inc., v. Waterman S.S. Corp.*, 333 U.S. 103 (1948)). In *Chicago & Southern Airlines*, the Court firmly stated:

[T]he very nature of executive decisions as to foreign policy is political, not judicial. Such decisions are wholly confided by our Constitution to the political departments of the government, Executive and Legislative. They are delicate, complex, and involve large elements of prophecy. They are and should be undertaken only by those directly responsible to the people whose welfare they advance or imperil. They are decisions of a kind for which the Judiciary has neither aptitude, facilities nor responsibility and which has long been held to belong in the domain of political power not subject to judicial intrusion or inquiry.

Chicago & S. Airlines, Inc., 333 U.S. at 111 (citing *Coleman v. Miller*, 307 U.S. 433, 454 (1939); *United States v. Curtiss-Wright Corp.*, 299 U.S. 304, 319–21 (1936); *Oetjen*, 246 U.S. at 302).

⁶⁷ See generally *infra* notes 68–74 and accompanying text.

⁶⁸ *Rappenecker v. United States*, 509 F. Supp. 1024, 1028 (N.D. Cal. 1980) (citing *Williams v. Suffolk Ins. Co.*, 38 U.S. (13 Pet.) 415, 419–20 (1839)). Such determinations made by the President are “not subject to judicial scrutiny.” *Id.*

⁶⁹ *Bentzlin v. Hughes Aircraft Co.*, 833 F. Supp. 1486, 1497 (C.D. Cal. 1993) (“[t]he policy decisions made in war are clearly beyond the competence of the courts to review . . .”); *Tiffany v. United States*, 931 F.2d 271, 277 (4th Cir. 1991) (“Of the legion of governmental endeavors, perhaps the most clearly marked for judicial deference are provisions for national security and defense. The decisions whether and under what circumstances to employ military force are constitutionally reserved for the executive and legislative branches.”) (citations omitted).

control of the political branches.⁷⁰ Tort suits that challenge the internal operations of these areas of the military are likely to be dismissed as political questions.⁷¹ As one court succinctly stated, “[t]he judicial branch is by design the least involved in military matters. . . . Even apart from matters of constitutional text, the reservation of judicial judgment on strictly military matters is sound policy.”⁷² Lacking the electoral accountability of the other two branches, the Judicial Branch is ill-suited to make decisions regarding the employment of military forces.⁷³ Even though courts have now backed off the sweeping dicta of the early cases, one constant has prevailed: “[t]he strategy and tactics employed on the battlefield are clearly not subject to judicial review.”⁷⁴

Notwithstanding the foregoing prohibitions on judicial conduct, the Supreme Court has cautioned, “it is error to suppose that every case or controversy which touches foreign relations lies beyond judicial cognizance.”⁷⁵ As mentioned earlier, vast precedent exists for judicial involvement in foreign and military affairs.⁷⁶ Case law establishes that military decisions *are* reviewable by federal courts.⁷⁷ An assertion of

⁷⁰ *Gilligan v. Morgan*, 413 U.S. 1, 10 (1973); *see Carmichael v. Kellogg Brown & Root Serv., Inc.*, No. 08-14487, 2009 U.S. App. LEXIS 14237, at *39 (11th Cir. Jun. 30, 2009) (holding that military decisions “pertain[ing] to battlefield or combat activities . . . are paradigmatically insulated from judicial review.”).

⁷¹ *Aktepe v. United States*, 105 F.3d 1400, 1403 (11th Cir. 1997) (“The Supreme Court has generally declined to reach the merits of cases requiring review of military decisions, particularly when those cases challenged the institutional functioning of the military in areas such as personnel, discipline, and training.”) (citing *Chappell v. Wallace*, 462 U.S. 296, 304 (1983); *Gilligan*, 413 U.S. at 5–13; *Orloff v. Willoughby*, 345 U.S. 83, 90–92 (1953)).

⁷² *Tozer v. LTV Corp.*, 792 F.2d 403, 405 (4th Cir. 1986).

⁷³ *Id.* (contending that it would not be “seemly” for “a democracy’s most serious decisions, those providing for common survival and defense, [to] be made by its least accountable branch of government”).

⁷⁴ *Tiffany*, 931 F.2d at 277 (citing *DaCosta v. Laird*, 471 F.2d 1146, 1155–56 (2d Cir. 1973)).

⁷⁵ *Baker v. Carr*, 369 U.S. 186, 211 (1963); *see Suhail Najim Abdullah Al Shimari v. CACI Premier Tech., Inc.*, No. 1:08CV827 (GBL), 2009 U.S. Dist LEXIS 29995, at *27 (E.D. Va. Mar. 18, 2009) (“[M]atters are not beyond the reach of the judiciary simply because they touch upon war or foreign affairs.”) (citing *Hamdan v. Rumsfeld*, 548 U.S. 557 (2006); *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004); *Dames & Moore v. Regan*, 453 U.S. 654 (1981); *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952); *United States v. Lindh*, 212 F. Supp. 2d 541 (E.D. Va. 2002)).

⁷⁶ *See supra* note 63 and accompanying text.

⁷⁷ *Koohi v. United States*, 976 F.2d 1328, 1331 (9th Cir. 1992) (“The Supreme Court has made clear the federal courts are capable of reviewing military decisions”) (citing *The Paquete Habana*, 175 U.S. 677 (1900); *Scheuer v. Rhodes*, 416 U.S. 232 (1974)); *see Developments, supra* note 52, at 1199.

military necessity, standing alone, is not a bar to judicial action.⁷⁸ Merely because a dispute can be tied in some way to combat activities does not prevent a court from reviewing it.⁷⁹ Although an action arises in a contingency environment, if a case is essentially “an ordinary tort suit” it is well within the competence of the courts to entertain.⁸⁰ Courts have underscored the point: no litmus test exists that prohibits judicial action merely because an issue involves the military in some fashion.

Where plaintiffs seek only damages and not injunctive relief, such cases are “particularly judicially manageable.”⁸¹ When such a damages-only lawsuit concerns only a defense contractor (as opposed to the Federal Government), courts have held that such actions do not involve “overseeing the conduct of foreign policy or the use and disposition of military power.”⁸² Thus, those actions are less likely to raise political

[T]here can be no doubt that the Constitution places primary power to conduct foreign relations in the executive branch. Nevertheless, the Constitution grants unreviewable authority only in tightly defined areas—never for the entire swath of “foreign relations.” In the absence of extenuating circumstances, litigation that carries the simple possibility (or probability, or even certainty) of impeding one of the Executive’s international relations interests is no less justiciable than litigation that might impede, say, one of its domestic regulatory interests. Because both the Constitution and Congress can constrain the Executive’s pursuit of its interests, the judiciary must be ready to judge those interests if it aims to act as a meaningful check on the Executive’s power.

Id. (footnotes omitted).

⁷⁸ *Koohi*, 976 F.2d at 1331.

⁷⁹ *Ibrahim v. Titan Corp.*, 391 F. Supp. 2d 10, 15 (D.D.C. 2005) (“The Constitution’s allocation of war powers to the President and Congress does not exclude the courts from every dispute that can arguably be connected to ‘combat[]’”) (citing *Hamdi*, 542 U.S. at 526–38).

⁸⁰ *Linder v. Portocarrero*, 963 F.2d 332, 337 (11th Cir. 1992) (“[T]he common law of tort provides clear and well-settled rules on which the district court can easily rely”) (citing *Klinghoffer v. S.N.C. Achille Lauro*, 937 F.2d 44, 49 (2d Cir. 1991)); see *McMahon v. Presidential Airways, Inc.*, 502 F.3d 1331, 1364 (11th Cir. 2007) (“The flexible standards of negligence law are well-equipped to handle varying fact situations.”).

⁸¹ *Koohi*, 976 F.2d at 1332 (“Damage actions are particularly judicially manageable. By contrast, because the framing of injunctive relief may require the courts to engage in the type of operational decision-making beyond their competence and constitutionally committed to other branches, such suits are far more likely to implicate political questions.”).

⁸² *Ibrahim*, 391 F. Supp. 2d at 15 (D.D.C. 2005) (citing *Luftig v. McNamara*, 373 F.2d 664, 666 (D.C. Cir. 1967)); see *Suhail Najim Abdullah Al Shimari v. CACI Premier*

questions than suits against the Government, suits seeking injunctive relief, or both.

Although courts have now generally rejected their earlier tendency to liberally apply the doctrine in any case touching foreign affairs or the military, courts still hesitate to question executive policy on foreign affairs and military decisions made on the battlefield. Regardless, courts today *will* entertain combat zone tort actions provided such actions stop short of infringing on prohibited areas of military operations.

V. Recent Developments in the Political Question Doctrine: The GWOT Cases

Given the enormous amount of money involved in Government contingency contracting⁸³ and the correspondingly large number of contractors and contractor employees performing GWOT contingency contracts,⁸⁴ the number of plaintiffs seeking redress for tortious conduct was certain to rise—and it did.⁸⁵ Universally, defendant defense contractors invoked the political question doctrine in order to shield

Tech., Inc., No. 1:08CV827 (GBL), 2009 U.S. Dist. LEXIS 29995, at *17 (E.D. Va. Mar. 18, 2009) (contending “a key distinction” exists when the defendant is a private party as opposed to the Government).

⁸³ The U.S. Government Accountability Office (GAO) reports the Department of Defense (DoD), the Department of State, and U.S. Agency for International Development “obligated at least \$33.9 billion during fiscal year 2007 and the first half of fiscal year 2008 on 56,925 contracts with performance in either Iraq or Afghanistan.” U.S. GOV’T ACCOUNTABILITY OFFICE, REP. NO. 09-19, CONTINGENCY CONTRACTING: DOD, STATE AND USAID CONTRACTS AND CONTRACTOR PERSONNEL IN IRAQ AND AFGHANISTAN 5 (2008) [hereinafter GAO REP.]. Approximately 90% of this amount was obligated to DoD contracts. *Id.* at summary. Furthermore, with President Obama’s decision to leave combat troops in Iraq until August 2010, and logistics and supply forces there for longer (possibly until 31 December 2011), coupled with his stated desire to increase combat troop strength in Afghanistan, there is no indication the government’s commitment to contingency contracting in support of the missions in Iraq and Afghanistan will soon wane. *See generally* Dan Lothian & Suzanne Malveaux, *Obama: U.S. to Withdraw Most Iraq Troops by August 2010*, CNN.COM, Feb. 27, 2009, <http://www.cnn.com/2009/POLITICS/02/27/obama.troops/index.html>; Paul Steinhauser, *Poll: Most Support Plan to Bolster U.S. Troops in Afghanistan*, CNN.COM, Feb. 26, 2009, <http://www.cnn.com/2009/POLITICS/02/26/us.troops.poll/>.

⁸⁴ *See* GAO REP., *supra* note 83, at 6. As of April 2008, DoD had almost 200,000 contractor personnel in Iraq and Afghanistan. *Id.*

⁸⁵ *See generally infra* pp. 103–12.

themselves from liability in their performance of GWOT contracts,⁸⁶ some with more success than others.⁸⁷ The first significant case centered around the tragic events at the Abu Ghraib prison in Iraq.⁸⁸

In *Ibrahim v. Titan Corp.*, Iraqi plaintiffs alleged they were tortured, raped, humiliated, beaten, and starved while in U.S. custody.⁸⁹ Apparently fearing a dismissal on sovereign immunity grounds if they sued the U.S. Government, the plaintiffs instead chose to name as defendants the contractors who provided interpreters and interrogators for the prison.⁹⁰ The defendants filed a motion to dismiss, alleging the matter involved political questions.⁹¹ The court held the case should not be dismissed at such an early stage on political question grounds, especially because the United States was not a party to the case.⁹² *Ibrahim* is significant because it was the first GWOT case to underscore the need for full factual development of a case prior to an assessment of justiciability.

Beginning with *Fisher v. Halliburton, Inc.*,⁹³ district courts heard a series of cases involving injuries sustained from convoy operations in Iraq in 2004.⁹⁴ In *Fisher*, the plaintiffs were civilian truck drivers providing transportation services for Kellogg Brown & Root (KBR)⁹⁵ under the U.S. Army's Logistics Civil Augmentation Program (LOGCAP) contract.⁹⁶ While following the Army's local Iraqi guide,

⁸⁶ See generally Addicott, *supra* note 7, at 351 (“[S]ince the case can be disposed of as non-justiciable, defense counsel representing a subject contracting company invariably include the political question doctrine either as a pre-answer motion or as an integral part of the responsive pleading.”).

⁸⁷ See generally *infra* pp. 103–12.

⁸⁸ *Ibrahim v. Titan Corp.*, 391 F. Supp. 2d 10 (D.D.C. 2005).

⁸⁹ *Id.* at 12.

⁹⁰ *Id.*

⁹¹ *Id.* at 12–13.

⁹² *Id.* at 16.

⁹³ 454 F. Supp. 2d 637 (S.D. Tex. 2006), *rev'd sub nom.*, *Lane v. Halliburton*, 529 F.3d 548 (5th Cir. 2008).

⁹⁴ *Id.*; see generally *infra* pp. 103–06.

⁹⁵ At the time, KBR was a subsidiary of Halliburton. See Kelly Kennedy, *Suit Alleges KBR, Halliburton Misconduct at Balad*, ARMY TIMES, Dec. 15, 2008, at 31 (“Halliburton announced in April 2007 that it had dissolved ties with KBR, which had been its contracting, engineering and construction unit since the 1960s.”).

⁹⁶ *Fisher v. Halliburton, Inc.*, 454 F. Supp. 2d 637, 638–39 (S.D. Tex. 2006), *rev'd sub nom.*, *Lane v. Halliburton*, 529 F.3d 548 (5th Cir. 2008); see U.S. DEP'T OF ARMY, REG. 700-137, LOGISTICS CIVIL AUGMENTATION PROGRAM (LOGCAP) (16 Dec. 1985).

plaintiffs' convoy suffered an attack by anti-American forces and several members were killed and injured.⁹⁷ Plaintiffs subsequently filed suit, alleging negligence in KBR's operation of the convoy and fraudulence in the contractor's representations of a "safe work environment."⁹⁸ Claiming plaintiffs' allegations were barred by the political question doctrine, KBR filed a motion to dismiss alleging the Army controlled convoy deployment and protection, and that any decisions made by KBR were inextricably "interwoven" with those of the Army.⁹⁹ The court analyzed the competing allegations using the *Baker* criteria.

In addressing the first *Baker* criterion, the *Fisher* court broadly stated "war and foreign policy are the provenance of the Executive," and even more broadly proclaimed "courts have consistently held that issues involving war, and actions taken during war, are beyond judicial competence."¹⁰⁰ Despite the previously discussed precedent to the contrary,¹⁰¹ the court held it could not "try a case set on a battlefield during war-time without an impermissible intrusion into powers expressly granted to the Executive by the Constitution."¹⁰² Given the long history of judicial involvement in foreign and military affairs, these statements are overbroad and unsupported by the weight of political question law. Nonetheless, the *Fisher* court found the first *Baker* criterion implicated.¹⁰³

In a holding more consistent with precedent, the court found the second *Baker* criterion implicated because the Army was responsible for

The LOGCAP objective is to preplan for the use of civilian contractors to perform selected services in wartime to augment Army forces. Utilization of civilian contractors in a theater of operation will release military units for other missions or fill shortfalls. This provides the Army with an additional means to adequately support the current and programmed force.

Id. para. 1-1; *see also* Harris v. Kellogg, Brown & Root Servs., Inc., No. 08-563, 2009 U.S. Dist LEXIS 26547, at *4-5 (W.D. Pa. Mar. 31, 2009) (explaining the implementation of the LOGCAP contract in the Iraq and Afghanistan theater of operations).

⁹⁷ *Fisher*, 454 F. Supp. 2d at 639.

⁹⁸ *Lane*, 529 F.3d at 555 (referencing the facts of *Fisher*).

⁹⁹ *Fisher*, 454 F. Supp. 2d at 639.

¹⁰⁰ *Id.* at 641.

¹⁰¹ *See supra* notes 63, 75-82, and accompanying text.

¹⁰² *Fisher*, 454 F. Supp. 2d at 641.

¹⁰³ *Id.*

the security, intelligence, and route selection of the convoy operations.¹⁰⁴ Thus, any inquiry into causation regarding the plaintiffs' injuries would require judicial examination of the Army's decisions in these areas—something courts lack standards to accomplish.¹⁰⁵ After finding the second *Baker* criterion implicated, the court speculated that in order to resolve the matter it may need to question the wisdom of the Executive's policies of convoy operations and employment of civilian contractors in a combat zone. Because of the likelihood of this prohibited task, the court found the third *Baker* criterion implicated as well.¹⁰⁶

In another KBR LOGCAP convoy case from 2004, *Whitaker v. Kellogg Brown & Root*, a U.S. Soldier was killed due to the alleged negligence of a KBR driver.¹⁰⁷ KBR filed a motion to dismiss, claiming the matter “turn[ed] on strategic and tactical military decisions made in a combat zone.”¹⁰⁸ The court based its conclusion that a political question existed on the non-GWOT case of *Aktepe v. United States*,¹⁰⁹ which did not involve a defense contractor defendant.¹¹⁰ Nonetheless, the court held “the same principles apply[,]” and “a soldier injured at the hands of a contractor which is performing military functions subject to the military's orders and regulations also raises the same political questions” as if the Government were the defendant.¹¹¹ As such, the *Whitaker* court

¹⁰⁴ *Id.* at 642.

¹⁰⁵ *Id.* at 643.

In order to hear this case, the court would have to substitute its judgment for that of the Army. For example, the court would need to determine what intelligence the Army gave to KBR about the route, whether that intelligence was sufficient, what forces were deployed with the convoys, whether they were sufficient, and whether they performed properly. Even if KBR had authority to deploy or recall the convoys, the court would still need to determine whether the Army could or should have countermanded that order. No judicial standards exist for making these determinations.

Id. (footnote omitted).

¹⁰⁶ *Id.* at 644.

¹⁰⁷ *Whitaker v. Kellogg Brown & Root, Inc.*, 444 F. Supp. 2d 1277, 1278 (M.D. Ga. 2006).

¹⁰⁸ *Id.* In support of its contention, KBR relied on “Army regulations regarding convoy operations and the use of civilian contractors.” *Id.* at 1278–79.

¹⁰⁹ 105 F.3d 1400 (11th Cir. 1997).

¹¹⁰ *Aktepe v. United States*, 105 F.3d 1400 (11th Cir. 1997); *Whitaker*, 444 F. Supp. 2d at 1281 (“The Court recognizes that the claims in *Aktepe* were against the United States and not a government contractor.”).

¹¹¹ *Whitaker*, 444 F. Supp. 2d at 1281.

found both the first and second *Baker* criteria implicated and granted defendant KBR's motion to dismiss.¹¹²

In *Lessin v. Kellogg Brown & Root*,¹¹³ another Army Soldier was injured on convoy duty due to the alleged negligence of KBR employees. The defense contractor alleged this case "involve[d] a political question of the military's decision-making in combat scenarios."¹¹⁴ The court conceded "where the military's strategy, decision-making, or orders are necessarily bound up with the claims asserted in a case, the political question doctrine is implicated, and the case is inappropriate for judicial inquiry."¹¹⁵ However, the court found that the facts were not yet developed enough in this case to indicate the presence of a political question and denied KBR's motion to dismiss.¹¹⁶ The court added that this incident was "essentially, a traffic accident" and "[c]laims of negligence arising from this type of incident are commonly adjudicated by courts, using well-developed judicial standards."¹¹⁷ *Lessin* underscored the importance of a plaintiff's ability to untangle allegations regarding a contractor's actions from the actions and decisions of the military.

The principles set forth in *Lessin* also proved persuasive to other district courts. In *Carmichael v. Kellogg Brown & Root Services, Inc.*,¹¹⁸ a subsequent convoy case in which the plaintiff was an Army Soldier injured due to the alleged negligence of KBR, the court chose to follow the holding of *Lessin* rather than *Whitaker*.¹¹⁹ The *Carmichael* court claimed that *Lessin* "best states the test"¹²⁰ for such cases: "plaintiff's claims are barred by the political question doctrine if 'military decision-making or policy would be a necessary inquiry, inseparable from the claims asserted.'"¹²¹ Viewed together, the convoy cases underscore the

¹¹² *Id.* at 1281–82. This case was not appealed. *Lane v. Halliburton*, 529 F.3d 548, 568 n.9 (5th Cir. 2008).

¹¹³ No. H-05-01853, 2006 U.S. Dist. LEXIS 39403 (S.D. Tex. June 12, 2006).

¹¹⁴ *Lessin v. Kellogg Brown & Root*, 2006 U.S. Dist. LEXIS 39403, at *2.

¹¹⁵ *Id.* at *8.

¹¹⁶ *Id.* at *15.

¹¹⁷ *Id.* at *8.

¹¹⁸ 450 F. Supp. 2d 1373 (N.D. Ga. 2006).

¹¹⁹ *Id.* at 1376.

¹²⁰ *Id.* at 1375; *see also* *Harris v. Kellogg, Brown & Root Servs., Inc.*, No. 08-563, 2009 U.S. Dist. LEXIS 26547, at *62 (W.D. Pa. Mar. 31, 2009) (finding *Lessin* "particularly persuasive").

¹²¹ *Carmichael*, 450 F. Supp. 2d at 1375 (quoting *Lessin v. Kellogg Brown & Root*, 2006 U.S. Dist. LEXIS 39403, at *7). Following the completion of discovery in this case the

requirement for a connection to *military* decision-making or policy prior to dismissal on political questions grounds.

*Smith v. Halliburton*¹²² was another significant GWOT district court case decided prior to the input of the appellate courts. The case involved an allegation of negligence against a defense contractor charged with operating a dining facility in Iraq pursuant to LOGCAP.¹²³ In December 2004, a suicide bomber infiltrated the dining facility at a forward operating base (FOB) in Mosul, Iraq, and detonated explosives, killing twenty-three people and wounding sixty-two.¹²⁴ Plaintiffs alleged defendants failed to properly secure the mess tent, despite repeated warnings that attacks were likely to occur.¹²⁵ The *Smith* court held the first *Baker* criterion was implicated because the military, not the contractor, was responsible for force protection at the FOB.¹²⁶ “[a]llowing this action to proceed would require the court to substitute its judgment on military decision-making for that of the branches of government entrusted with this task.”¹²⁷ The court also found the second and third *Baker* criteria were implicated, holding that it lacked the standards to determine what adequate force protection measures should have been¹²⁸ and that “[p]olicy determinations involving force protection measures in a hostile area of Iraq are clearly not appropriate for judicial determination.”¹²⁹ The district court granted the defendants’ motion to dismiss.¹³⁰ *Smith* reinforces the previously discussed convoy cases’ theme that certain military policy matters are off limits to judicial discretion.

In 2004, three U.S. Army Soldiers serving in Afghanistan were killed when the aircraft in which they were passengers crashed into a

defendant contractor again moved to dismiss and the motion was granted. Carmichael v. Kellogg Brown & Root Servs., Inc., 564 F. Supp 2d 1363 (N.D. Ga. 2008), *aff’d* No. 08-14487, 2009 U.S. App. LEXIS 14237 (11th Cir. June 30, 2009).

¹²² No. H-06-0462, 2006 U.S. Dist. LEXIS 61980 (S.D. Tex. Aug. 30, 2006).

¹²³ *Id.* at *2–5.

¹²⁴ *See Smith*, 2006 U.S. Dist. LEXIS 30530, at *2–3.

¹²⁵ *Id.* at *3–4.

¹²⁶ *Smith*, 2006 U.S. Dist. LEXIS 61980, at *15.

¹²⁷ *Id.* at *23. The court added, “[t]he control of access to a military base is clearly within the constitutional powers granted to both Congress and the President.” *Id.* at *24 (citing Cafeteria & Rest. Workers Union v. McElroy, 367 U.S. 886, 890 (1961)).

¹²⁸ *Smith*, 2006 U.S. Dist. LEXIS 61980, at *24–25.

¹²⁹ *Id.* at *26.

¹³⁰ *Id.* at *28. This case was not appealed. Lane v. Halliburton, 529 F.3d 548, 568 (5th Cir. 2008).

mountain.¹³¹ A defense contractor owned and operated the aircraft.¹³² In the case of *McMahon v. Presidential Airways, Inc.*, the plaintiffs brought wrongful death actions against the contractor alleging negligence in the equipment and operation of the aircraft.¹³³ Under the statement of work of the contract,¹³⁴ the contractor was required to furnish the aircraft, flight personnel, maintenance, and supervision for the air transportation services, while the military “directed what missions would be flown, when they would be flown, and what passengers and cargo would be carried.”¹³⁵ Prior to denying the defendant’s motion to dismiss on political question grounds,¹³⁶ the district court invited the U.S. Government to intervene—the Government declined.¹³⁷ The contractor appealed the denial of this motion to the United States Court of Appeals for the Eleventh Circuit.¹³⁸ The Eleventh Circuit addressed the political question issue by applying the *Baker* criteria.

As to the analysis of the first *Baker* criterion, the court held the defendant to a “double burden” because the case involved a private contractor and not the U.S. Government.¹³⁹ In order to show the matter

¹³¹ *McMahon v. Presidential Airways, Inc.*, 502 F.3d 1331, 1336 (11th Cir. 2007).

¹³² The court dismissed the claims against one defendant contractor on jurisdictional grounds. *Id.* at 1336 n.2. The court then referred to the remaining defendants collectively as “Presidential.” *Id.* at 1336. Presidential owned and operated the plane. *Id.* Presidential was under contract with the military “to provide air transportation and other support services in aid of the military mission in Afghanistan.” *Id.*

¹³³ *Id.* at 1337. Both pilots were employees of Presidential. *Id.* at 1336 n.1.

¹³⁴ A statement of work is:

[t]he portion of a contract that describes the actual work to be done by means of (1) specifications or other minimum requirements, (2) quantities, (3) performance dates, (4) time and place of performance of services, and (5) quality requirements It plays a key role in the solicitation because it serves as the basis for the contractor’s response. It also serves as a baseline against which progress and subsequent contractual changes are measured during contract performance.

RALPH C. NASH, JR. ET AL., *THE GOVERNMENT CONTRACTS REFERENCE BOOK* 492 (2d ed. 1998).

¹³⁵ *McMahon*, 502 F.3d at 1336.

¹³⁶ *Id.* at 1337–38. Prior to denying defendant’s motion to dismiss, the district court also considered defendant’s *Feres* immunity claim and preemption claim under the Federal Tort Claims Act. *Id.*

¹³⁷ *Id.* at 1337 n.4.

¹³⁸ *Id.* at 1338.

¹³⁹ *Id.* at 1359–60.

was textually committed to the political branches, first the contractor would need to demonstrate that adjudication of the issue would require the court to reexamine a *military* decision, then the contractor must prove that such military decision was “insulated from judicial review.”¹⁴⁰ The court found the contractor could not meet the first part of this test based on the limited factual development in the case thus far¹⁴¹ but noted the statement of work gave the contractor “general responsibility for making the decisions regarding the flights it provided” to the military.¹⁴² The contractor failed to meet its burden under the first *Baker* criterion.¹⁴³

With the second *Baker* criterion, the *McMahon* court held that the defendant failed to show the case would require the court to resort to judicially undiscoverable or unmanageable standards.¹⁴⁴ The court found it significant that the plaintiffs’ allegations of contractor negligence did not “involve combat, training activities, or any peculiarly *military* activity at all.”¹⁴⁵ Absent a reexamination of any military decision, “[i]t is well within the competence of a federal court to apply negligence standards to a plane crash.”¹⁴⁶ Furthermore, the court also found significance in the U.S. Government’s election not to intervene in the case¹⁴⁷ as well as the fact that the suit sought only damages, not

¹⁴⁰ *Id.* at 1360.

¹⁴¹ *Id.*

¹⁴² *Id.* The court found that the statement of work gave the military only “discrete” areas of control. *Id.* at 1361. None of those discrete areas appeared to be implicated by plaintiff’s allegations. *Id.*

¹⁴³ *Id.* at 1360–63.

¹⁴⁴ *Id.* at 1363.

¹⁴⁵ *Id.*

¹⁴⁶ *Id.* at 1364.

[F]lying over Afghanistan during wartime is different from flying over Kansas on a sunny day. But this does not render the suit inherently non-justiciable. While the court may have to apply a standard of care to a flight conducted in a less than hospitable environment, that standard is not inherently unmanageable. . . . The flexible standards of negligence law are well-equipped to handle varying fact situations. The case does not involve a *sui generis* situation such as military combat or training, where courts are incapable of developing judicially manageable standards.

Id. (citations and footnotes omitted).

¹⁴⁷ *Id.* at 1365.

injunctive relief.¹⁴⁸ The Eleventh Circuit affirmed the denial of defendant's motion to dismiss.¹⁴⁹

In *Lane v. Halliburton*,¹⁵⁰ the United States Court of Appeals for the Fifth Circuit weighed in on the political question issue through its consolidated opinion involving three LOGCAP convoy cases, including *Fisher v. Halliburton*,¹⁵¹ discussed earlier.¹⁵² All three cases involved allegations of fraud against KBR in guaranteeing the safety of its convoy operations in Iraq¹⁵³ and negligence in allowing the convoys to proceed on the specific dates the convoys were attacked.¹⁵⁴ The district court¹⁵⁵ had previously dismissed all three cases with prejudice, finding political questions present.¹⁵⁶ The *Lane* court framed the issue as follows: “[W]ould resolving the Plaintiffs’ tort-based legal claims invariably require analyzing the Executive’s war-time decision-making, or do KBR’s actions and motives form the sole issues?”¹⁵⁷ Not surprisingly, the court based its analysis on the *Baker* criteria.

Regarding the first *Baker* criterion, the court cited *McMahon’s* “double burden”¹⁵⁸ that first requires a defendant contractor to show a *military* decision will need to be reexamined.¹⁵⁹ Holding this instance to be a “matter[] of tort-based compensation,” the court found no textual commitment of this matter to other branches of government.¹⁶⁰ As in

¹⁴⁸ *Id.* at 1364.

¹⁴⁹ *Id.* at 1366.

¹⁵⁰ 529 F. 3d 548 (5th Cir. 2008). *Lane* is the case contemplated by the Nash & Cibinic Report mentioned earlier. NASH & CIBINIC REP., *supra* note 5, ¶ 44.

¹⁵¹ *Lane* also consolidated two other factually similar cases. *Smith-Idol v. Halliburton*, No. H-06-1168, 2006 U.S. Dist. LEXIS 75574 (S.D. Tex. Oct. 11, 2006), *rev’d sub nom.*, *Lane v. Halliburton*, 529 F.3d 548 (5th Cir. 2008); *Lane v. Halliburton*, No. 11-06-1971, 2006 U.S. Dist. LEXIS 63948 (S.D. Tex. Sept. 7, 2006), *rev’d*, *Lane v. Halliburton*, 529 F.3d 548 (5th Cir. 2008).

¹⁵² See *supra* notes 95–106 and accompanying text.

¹⁵³ *Lane*, 529 F. 3d at 555 (“The essence of these claims is that KBR utilized intentionally misleading and false advertisements and recruiting materials to induce Plaintiffs to accept employment with KBR and relocate to Iraq.”).

¹⁵⁴ *Id.*

¹⁵⁵ The same district court judge presided over all three cases.

¹⁵⁶ *Id.* at 554.

¹⁵⁷ *Id.* at 557.

¹⁵⁸ See *supra* notes 139–40, and accompanying text.

¹⁵⁹ The *Lane* court held this was necessary because “KBR is not part of a coordinate branch of the federal government.” *Lane*, 529 F. 3d at 560.

¹⁶⁰ *Id.*

McMahon, the contractor in *Lane* was unable to meet its burden under the first *Baker* criterion.¹⁶¹

As to the second *Baker* criterion, the court found it to be “arguably the most critical factor in the political question analysis . . . because at least some of the allegations would draw a court into a consideration of what constituted adequate force protection for the convoys.”¹⁶² Central to this issue was the negligence element of causation. If a court will need to explore the military’s role as to causation, a political question problem “will loom large.”¹⁶³ The court held plaintiffs’ fraud claims were less likely to invoke political question problems as to causation¹⁶⁴ than would plaintiffs’ negligence claims.¹⁶⁵ The second *Baker* criterion was not implicated.¹⁶⁶

With the third *Baker* criterion, the *Lane* court found the prohibition on nonjudicial policy determinations likely inapplicable, holding “[t]he court will be asked to judge KBR’s policies and actions, not those of the military or Executive Branch.”¹⁶⁷ With no *Baker* criteria implicated, the court reversed and remanded the district court opinions. It concluded that, at least at this early stage of the litigation, political questions were not present.¹⁶⁸

¹⁶¹ *Id.*

¹⁶² *Id.*

¹⁶³ *Id.* at 561.

¹⁶⁴ *Id.* at 567 (“[T]he cases might be triable without raising a political question because the court could assess KBR’s liability by simply being aware of the information the military provided to KBR, not second-guessing that information.”).

¹⁶⁵ *Id.*

Proving KBR’s negligent breach of a duty in Iraq not to allow a convoy to proceed if conditions were too dangerous will involve rather different evidence than would proof of misrepresentations made during hiring or later about safety. . . . [A]t some point the political question analysis between the two will likely diverge. The Plaintiffs’ negligence allegations move precariously close to implicating the political question doctrine, and further factual development very well may demonstrate that the claims are barred.

Id.

¹⁶⁶ *Id.* at 563.

¹⁶⁷ *Id.*

¹⁶⁸ *Id.* at 568–69.

McMahon and *Lane* remain the prominent cases on point. To date, only one appellate court has upheld a political question dismissal of a tort suit based on the combat zone conduct of defense contractors or their employees.¹⁶⁹ Since *McMahon* and *Lane*, more district courts have faced these issues.¹⁷⁰ Based on the particular facts presented in each case, all held the political question doctrine did not serve as a bar to suit.¹⁷¹ From the initial GWOT district court cases through *McMahon*, *Lane* and beyond, defense contractors accused of tortious combat zone conduct continue to regularly invoke the doctrine in an attempt to avoid liability.

VI. Lessons Learned from the GWOT Cases: The Current Test for Political Questions

By applying traditional political question doctrine principles to modern combat zone realities, *McMahon*, *Lane*, and the other GWOT cases set forth a workable framework for courts to use in applying the political question test to current cases. The analysis begins generally with the *Baker* criteria—the presence of any one of which will result in a

¹⁶⁹ See *Carmichael v. Kellogg Brown & Root Serv., Inc.*, No. 08-14487, 2009 U.S. App. LEXIS 14237 (11th Cir. June 30, 2009). This convoy case distinguished both *McMahon* and *Lane*, citing the military's "plenary" control over the contractor's actions here as opposed to *McMahon*, the differing nature of the tortious allegations here as opposed to *Lane*, and the limited factual development of both. *Id.* at *47–52. The *Carmichael* court found the existence of a political question in large part because the court would have been required to examine military judgments. *Id.* at *24–25.

Because the circumstances under which the accident took place were so thoroughly pervaded by military judgments and decisions, it would be impossible to make any determination regarding [the defendants'] negligence without bringing those essential military judgments and decisions under searching judicial scrutiny. . . . [I]t is precisely this kind of scrutiny that the political question doctrine forbids.

Id.

¹⁷⁰ See, e.g., *Harris v. Kellogg, Brown & Root Servs., Inc.*, 2009 U.S. Dist. LEXIS 26547; *Flanigan v. Westwind Techs., Inc.*, 2008 U.S. Dist. LEXIS 82203; *Getz v. The Boeing Co.*, No. CV07-639CW, 2008 U.S. Dist. LEXIS 87557 (N.D. Cal. July 8, 2008); *Potts v. Dyncorp Int'l, LLC*, 465 F. Supp. 2d 1245 (M.D. Ala. 2006) (post-*McMahon*, pre-*Lane*).

¹⁷¹ See, e.g., *Harris v. Kellogg, Brown & Root Servs., Inc.*, 2009 U.S. Dist. LEXIS 26547; *Flanigan v. Westwind Techs., Inc.*, 2008 U.S. Dist. LEXIS 82203; *Getz v. The Boeing Company*, 2008 U.S. Dist. LEXIS 87557; *Potts v. Dyncorp Int'l, LLC*, 465 F. Supp. 2d 1245.

finding of a political question—and develops through its own specific application to defense contractor torts suits.

The analysis of the first *Baker* criterion, the textual commitment by the Constitution of a certain matter to one of the other Governmental branches, starts with an application of *McMahon's* “double burden” test.¹⁷² A defendant contractor must first show the plaintiff’s allegations require the court to question a *military* decision.¹⁷³ If the allegations would require only an assessment of the contractor’s own decisions or policies, this first prong of the test has not been established.¹⁷⁴ To satisfy the first half of this burden, a contractor must do more than merely allege a nexus between itself and the military¹⁷⁵ or broadly proclaim the Constitution delegates foreign policy or military matters to the political branches.¹⁷⁶ The contractor must offer concrete proof of the particular military decision called into question by the plaintiff’s allegations.¹⁷⁷ With the first portion of the double burden established, the defendant contractor must then show the particular military decision is insulated from judicial review.¹⁷⁸ The more control the military has over a contractor’s conduct the more likely a political question will present itself in the form of the first *Baker* criterion.¹⁷⁹

¹⁷² See *supra* notes 139–40, and accompanying text; *Lane*, 529 F. 3d at 560; *Flanigan*, 2008 U.S. Dist. LEXIS 82203, at *16; *Getz*, 2008 U.S. Dist. LEXIS 87557, at *18; *Potts*, 465 F. Supp. 2d at 1252.

¹⁷³ See *supra* note 139 and accompanying text; *Lane*, 529 F. 3d at 560; *Flanigan*, 2008 U.S. Dist. LEXIS 82203, at *16; *Getz*, 2008 U.S. Dist. LEXIS 87557, at *18; *Potts*, 465 F. Supp. 2d at 1252.

¹⁷⁴ *Potts*, 465 F. Supp. 2d at 1250–52.

¹⁷⁵ See *Addicott*, *supra* note 7, at 363 (“It is clear that the political question doctrine will not preclude judicial review simply because there exists some nexus between the contractor and the military.”); *id.* at 363 n.120 (“All contractors may lay claim to this nexus—they are, by definition, under contract with the government.”).

¹⁷⁶ See *Potts*, 465 F. Supp. 2d at 1248.

¹⁷⁷ See *McMahon v. Presidential Airways, Inc.*, 502 F.3d 1331, 1359–60 (11th Cir. 2007); *Lane*, 529 F. 3d at 560; *Flanigan*, 2008 U.S. Dist. LEXIS 82203, at *16; *Getz*, 2008 U.S. Dist. LEXIS 87557, at *18; *Potts*, 465 F. Supp. 2d at 1252.

¹⁷⁸ See *supra* note 140 and accompanying text. Examples of decisions courts have held to be insulated from judicial review include “‘core military decisions, including [military] communication, training, and drill procedures’ or ‘the strategy and tactics employed on the battlefield.’” *Carmichael v. Kellogg Brown & Root Servs.*, No. 1:06CV-507-TCB, 2008 U.S. Dist. LEXIS 52126, at *21–22 (N.D. Ga. July 8, 2008) (quoting *McMahon*, 502 F.3d at 1359).

¹⁷⁹ See *Potts*, 465 F. Supp. 2d at 1252 (“The courts in [*Smith and Whitaker*] emphasized the control that the United States had over the conduct at issue or the private parties themselves.”) (citing *McMahon v. Presidential Airways, Inc.*, 460 F. Supp. 2d 1315, 1320 (M.D. Fla. 2006), *aff’d* 502 F.3d 1331 (11th Cir. 2007)). See generally *Smith v.*

The second *Baker* criterion, which arises upon a lack of judicially manageable standards for resolving the issue, requires a determination of the standards that will be used to resolve the matter.¹⁸⁰ Will a court need to create standards based on the exigencies of combat or military policy and procedures?¹⁸¹ Federal courts are not equipped to evaluate the reasonableness of military decisions in combat.¹⁸² Such decisions result from “a complex, subtle balancing of many technical and military considerations, including the trade-off between safety and greater combat effectiveness.”¹⁸³ Or alternatively, does the matter merely involve an ordinary tort suit¹⁸⁴ that can be resolved simply by the application of well-established standards of tort-based compensation, which can be tailored “to account for the ‘less than hospitable environment’” of a combat zone?¹⁸⁵ Another key fact¹⁸⁶ regarding the second *Baker*

Halliburton, No. H-06-0462, 2006 U.S. Dist. LEXIS 61980 (S.D. Tex. Aug. 30, 2006); *Whitaker v. Kellogg Brown & Root, Inc.*, 444 F. Supp. 2d 1277 (M.D. Ga. 2006). For example, one district court noted that the GWOT district court cases which found the presence of political questions “each involved some form of active combat operations.” *Harris v. Kellogg, Brown & Root Servs., Inc.*, No. 08-563, 2009 U.S. Dist. LEXIS 26547, at *64 (W.D. Pa. Mar. 31, 2009) (citing *Smith v. Halliburton*, 2006 U.S. Dist. LEXIS 61980; *Carmichael v. Kellogg, Brown & Root Servs., Inc.*, 564 F. Supp. 2d 1363 (N.D. Ga. 2008); *Whitaker*, 444 F. Supp. 2d 1277; *Bentzlin v. Hughes Aircraft Co.*, 833 F. Supp. 1486 (C.D. Cal. 1993)).

¹⁸⁰ *Lane v. Halliburton*, 529 F. 3d 548, 560 (5th Cir. 2008) (“One of the most obvious limitations imposed by Article III, § 1, of the Constitution is that judicial action must be governed by *standard*, by *rule*.”) (quoting *Vieth v. Jubelirer*, 541 U.S. 267, 278 (2004)).

¹⁸¹ See *Getz*, 2008 U.S. Dist. LEXIS 87557, at *24 (“[C]ourts lack standards with which to judge whether reasonable care was taken to achieve tactical objectives in combat while minimizing injury and loss of life.”) (quoting *Zuckerbraun v. Gen. Dynamics Corp.*, 755 F. Supp. 1134, 1142 (D. Conn. 1990)).

¹⁸² See *McMahon*, 502 F.3d at 1363 (quoting *Gilligan v. Morgan* 413 U.S. 1 (1973); citing *Boyle v. United Techs. Corp.*, 487 U.S. 500 (1988)).

¹⁸³ *Getz*, 2008 U.S. Dist. LEXIS 87557, at *24 (quoting *Aktepe v. United States*, 105 F.3d 1400, 1404 (11th Cir. 1997)).

¹⁸⁴ *Id.* at *25 (quoting *Klinghoffer v. S.N.C. Achille Lauro*, 937 F.2d 44, 49 (2d Cir. 1991)).

¹⁸⁵ *Lane*, 529 F. 3d at 563 (quoting *McMahon*, 502 F.3d at 1363–64). In a subsequent district court case involving the electrocution of an Army Ranger due to a defective water pump in a shower at a base in Baghdad, the court expanded upon *McMahon*’s “Kansas” analogy discussed previously. *Harris v. Kellogg, Brown & Root Servs., Inc.*, No. 08-563, 2009 U.S. Dist. LEXIS 26547, at *75 (W.D. Pa. Mar. 31, 2009).

The Court recognizes that the standard of care to be applied in this matter raises unique issues and that providing maintenance services at a military base in Iraq is certainly different than providing the same at a civilian facility in Pennsylvania. However, these differences do not make the case non-justiciable. . . . The applicable duty owed by KBR to [the deceased Ranger], if any, can be defined with reference

criterion is whether a plaintiff seeks injunctive relief or only monetary damages—actions for damages are more judicially manageable.¹⁸⁷ Essentially, courts will avoid political question problems under the second criterion provided they rely on established judicial standards.

The third *Baker* criterion mandates a finding of a political question when a court cannot decide a case “without an initial policy determination of a kind clearly for nonjudicial discretion.”¹⁸⁸ Applying this criterion to GWOT contractor cases, “[t]he judiciary cannot announce policy positions on military readiness for which it is neither equipped nor, more importantly, constitutionally empowered to speak.”¹⁸⁹ To accomplish this element of review, one must determine if a court will need to second guess the policy determinations of the Executive or the military.¹⁹⁰ If so, a political question exists.¹⁹¹ Such impermissible policy determinations include judicial examination of the decision to go to war, the decision to hire contractors to perform traditional military missions in combat zones, and the manner in which

to common law negligence principles as well as [the contract and related service requests], and KBR’s internal operating procedures. While the Court cannot ignore the context in which the contract was performed, i.e., at a military base in Iraq, the reasonableness of KBR’s conduct can be evaluated in relation to any duty owed.

Id. (citing *McMahon*, 502 F.3d at 1363) (footnote omitted); *supra* note 146.

¹⁸⁶ *Getz*, 2008 U.S. Dist. LEXIS 87557, at *17 (“This fact . . . is relevant, but not dispositive.”).

¹⁸⁷ See *supra* note 81 and accompanying text; see also *McMahon*, 502 F.3d at 1364 n.34 (“[M]erely a suit for tort damages . . . is less likely to implicate the second *Baker* factor.”); *Harris*, 2009 U.S. Dist. LEXIS 26547, at *81 (“Plaintiffs seek compensation for [the decedent’s] injuries and death allegedly caused by KBR’s negligence. They do not seek to enjoin KBR’s conduct. This finding weighs in favor of judicial resolution.”).

¹⁸⁸ *Baker v. Carr*, 369 U.S. 186, 217 (1962); *Flanigan v. Westwind Techs., Inc.*, No. 07-1124, 2008 U.S. Dist. LEXIS 82203, at *23 (W.D. Tenn. Sept. 15, 2008) (“A political question under the third factor exists when, to resolve a dispute, the court must make a policy judgment of a legislative nature, rather than resolving the dispute through legal and factual analysis.”) (quoting *Gross v. German Found. Indus. Initiative*, 456 F.3d 363, 388 (3d Cir. 2006)).

¹⁸⁹ *Lane*, 529 F. 3d at 563.

¹⁹⁰ See *Flanigan*, 2008 U.S. Dist. LEXIS 82203, at *23 (“The court’s inquiry here focuses on ‘whether it will impermissibly intrude on the Executive’s role in formulating policy.’ In resolving cases, courts are not to ‘make initial policy decisions of a kind appropriately reserved for military discretion.’”) (quoting *Gross*, 456 F.3d at 389; *Aktepe v. United States*, 105 F.3d 1400, 1404 (11th Cir. 1997)); see also *Lane*, 529 F. 3d at 563.

¹⁹¹ See *Lane*, 529 F. 3d at 563.

contractors are utilized on the battlefield.¹⁹² On the other hand, if merely called upon to determine the negligence or otherwise tortious conduct of a contractor or its employees, the court is not in danger of exceeding the bounds of the third *Baker* criterion.¹⁹³

The fourth, fifth, and sixth *Baker* criteria generally do not significantly impact the disposition of a political question case unless a court's decision will "contradict prior decisions taken by a political branch in those limited contexts where such contradiction would seriously interfere with important governmental interests."¹⁹⁴ When they do arise, these issues usually present themselves intertwined with one or more of the first three criteria or they are merely raised in a conclusory fashion by defendant contractors.¹⁹⁵ As such, the final three *Baker* criteria are seldom case dispositive in and of themselves.

Several additional considerations arise outside of the framework of the *Baker* criteria. Due to the requirement for a "discriminating inquiry into the precise facts and posture"¹⁹⁶ of each political question case, courts should be reluctant to grant defense motions to dismiss at early stages of the litigation.¹⁹⁷ Rather, only when the facts of a case are fully developed can an accurate diagnosis of a political question be made.¹⁹⁸

¹⁹² See *Fisher v. Halliburton*, 454 F. Supp. 2d 637, 644 (S.D. Tex. 2006), *rev'd sub nom.* *Lane v. Halliburton*, 529 F.3d 548 (5th Cir. 2008); *Smith v. Halliburton*, No. H-06-0462, 2006 U.S. Dist. LEXIS 61980, at *25–26 (S.D. Tex. Aug. 30, 2006).

¹⁹³ *Potts v. Dyncorp Int'l, LLC*, 465 F. Supp. 2d 1245, 1254 (M.D. Ala. 2006) ("[W]hether [a contractor] acted negligently and wantonly [is] a decision that does not require an initial policy determination of a kind clearly for non-judicial discretion.").

¹⁹⁴ *Flanigan*, 2008 U.S. Dist. LEXIS 82203, at *24 (quoting *Norwood v. Raytheon Co.*, 455 F. Supp. 2d 597, 606 (W.D. Tex. 2006)).

¹⁹⁵ See *id.* In *Flanigan*, the defendants contended the last three *Baker* criteria were applicable, but did so only "in conclusory fashion, without presenting any case law or evidence supporting their assertions." *Id.* See generally *McMahon v. Presidential Airways, Inc.*, 502 F.3d 1331, 1364–65 (11th Cir. 2007).

¹⁹⁶ *Baker v. Carr*, 369 U.S. 186, 216 (1962).

¹⁹⁷ See generally *Lane*, 529 F.3d at 568; *McMahon*, 502 F.3d at 1365 n.36; *Carmichael v. Kellogg Brown & Root Servs.*, 450 F. Supp. 2d 1373, 1376 (N.D. Ga. 2006).

¹⁹⁸ Because the defendants in both *Lane* and *McMahon* sought to invoke the political question doctrine at such an early stage of the proceedings, the factual information considered by the district courts was more favorable to the plaintiffs than it likely would have been if raised later in the proceedings. See *Lane*, 529 F.3d at 557 ("In reviewing the dismissal order, we take the well-pled factual allegations of the complaint as true and view them in the light most favorable to the plaintiff."); *McMahon*, 502 F.3d at 1365 n.36; Addicott, *supra* note 7, at 363–64.

Furthermore, the involvement of the U.S. Government in a case should be considered a factor as well.¹⁹⁹ If the Executive Branch is invited to join the suit or otherwise provide its input and declines, the apparent lack of interest may signal a concession that the matter does not raise political questions.²⁰⁰ Though not dispositive by itself, this additional consideration should be viewed in conjunction with the other *Baker* criteria.

In summary, the current test for political questions in contingency contracting cases generally follows the *Baker* analysis. The first relevant issue in the political question analysis is whether a military decision is in question. If not, there can be no demonstration of textual commitment by the Constitution to the political branches. Even if a military decision is questioned, no political question problem presents itself unless the decision is insulated from judicial review. If traditional tort-based standards can be applied to adequately resolve the matter, the case will not fail for a lack of judicially manageable standards. However, if a court must create new standards that require it to judge the reasonableness of military conduct in combat, a political question will present itself. Courts likewise run afoul of the doctrine when they question Executive Branch policy determinations on the strategy and

[I]t is not surprising that the developing trend for dealing with motions to dismiss based on the political question doctrine is for the subject court to delay the determination until the close of discovery, when the fullest amount of information is available to measure against the Baker factors. Given the consequences of a non-justiciability finding, each side deserves the fullest opportunity to present all the facts at hand.

Id.

¹⁹⁹ See *McMahon*, 502 F.3d at 1365; *Harris v. Kellogg, Brown & Root Servs., Inc.*, No. 08-563, 2009 U.S. Dist. LEXIS 26547, at *84 (W.D. Pa. Mar. 31, 2009).

²⁰⁰ See *McMahon*, 502 F.3d at 1365; *Harris*, 2009 U.S. Dist. LEXIS 26547, at *84. However, some scholars question the wisdom of a judicial practice which uses executive branch interest in a case to gauge justiciability for political question purposes. See *Developments, supra* note 52, at 1200.

[B]y deferring to the Executive on the question of which suits it will hear, the judiciary is entrusting to the Executive its own duty to recognize violations of individuals' rights. . . . [W]hen the courts defer to the State Department's judgment on which cases should be dismissed, they entrust that institution with balancing both foreign relations concerns and access to the courts.

Id.

tactics of combat operations. One final take away from the GWOT political question cases: courts should be loath to grant motions to dismiss on political question grounds at early stages of litigation. The *Baker* criteria, if they exist, often do not present themselves until cases have undergone significant factual development.

VII. Other Defense Contractor Options: The Government Contractor Defense, Indemnification, and the Defense Base Act

Defense contractors frequently raise multiple defenses when sued over alleged torts committed in a contingency environment. The impact of potentially unfavorable²⁰¹ recent developments in the political question doctrine may be lessened when a contractor can complement its case with a more cogent defense argument or avoid a lawsuit altogether. Therefore, a brief discussion of these defenses and alternative courses of action is warranted.²⁰²

The Federal Tort Claims Act (FTCA) provides two prominent contractor defenses. Because the United States cannot be sued without a waiver of its sovereign immunity,²⁰³ the FTCA conveys a limited waiver

²⁰¹ See *supra* notes 5 and 11.

²⁰² Section VII is not intended to provide an exhaustive list of all possible contractor defenses or courses of action to avoid contingency-related tort suits. Rather, Section VII is intended to discuss several relevant alternatives which, in conjunction with the political question doctrine, could be avenues for defense contractor indemnification, reimbursement, immunity, or liability limitation. Other potentially viable alternatives not discussed in detail in Section VII include: the state secrets privilege, the Support Antiterrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act), and the Public Readiness and Emergency Preparedness Act (PREP Act). The state secrets privilege is “an evidentiary privilege that requires either the outright dismissal of a case or significant limitations on discovery where litigation would involve disclosure of important state secrets.” Holly Wells, *The State Secrets Privilege: Overuse Causing Unintended Consequences*, 50 ARIZ. L. REV. 967 (2008); *United States v. Reynolds*, 345 U.S. 1 (1953). The SAFETY Act provides limited immunity for “sellers (and purchasers) of qualified anti-terrorism technologies . . .”, Agnes P. Dover & Thomas L. McGovern III, *Risk Mitigation Approaches for Government Contractors* (07-5 Briefing Papers) 5 (Thomson & West 2007); 6 U.S.C. §§ 441–44 (2006). The PREP Act offers liability protections to “entities that produce and administer biological countermeasures . . .” Dover & McGovern, *supra*, at 7; 42 U.S.C.A. §§ 247d-6d, 247d-6e (LexisNexis 2009).

²⁰³ *Smith v. Halliburton*, No. H-06-0462, 2006 U.S. Dist. LEXIS 30530, at *15 (S.D. Tex. May 16, 2006) (citing *United States v. Mitchell*, 445 U.S. 535, 538 (1980)); *Fisher v. Halliburton*, 390 F. Supp. 2d 610, 614 (S.D. Tex. 2005) (citing *Loeffler v. Frank*, 486 U.S. 549, 554 (1988); *Zayler v. Dep’t of Agric. (In re Supreme Beef Processors, Inc.)*, 391 F.3d 629, 633 (5th Cir. 2004)).

under certain circumstances,²⁰⁴ with exceptions.²⁰⁵ The exceptions apply only to suits against the Federal Government, not Government contractors.²⁰⁶ However, in *Boyle v. United Technologies Corporation*,²⁰⁷ the Supreme Court held that the FTCA's discretionary function exception²⁰⁸ preempts, in certain situations, tort suits against defense contractors based on harm caused by design specifications in military equipment.²⁰⁹ This first exception, known as the Government

²⁰⁴ *Fisher*, 390 F. Supp. 2d at 614 (“The FTCA authorizes civil actions for damages against the United States for personal injury or death caused by the negligence of a government employee under circumstances in which a private person would be liable under the law of the state in which the negligent act or omission occurred.”) (quoting *Bursztajn v. United States*, 367 F.3d 485, 489 (5th Cir. 2004)).

²⁰⁵ *Lessin v. Kellogg Brown & Root*, No. H-05-01853, 2006 U.S. Dist. LEXIS 39403, at *10 (S.D. Tex. June 12, 2006) (citing 28 U.S.C. § 2674 (2006); *Quijano v. United States*, 325 F.3d 564, 567 (5th Cir. 2003)).

²⁰⁶ *Carmichael v. Kellogg Brown & Root Servs., Inc.*, 450 F. Supp. 2d 1373, 1377 (N.D. Ga. 2006); see *Lessin*, 2006 U.S. Dist. LEXIS 39403, at *10–11.

²⁰⁷ 487 U.S. 500 (1988).

²⁰⁸ 28 U.S.C. § 1346(b) (2006). Excepted from the Government's consent to suit is “[a]ny claim . . . based upon the exercise or performance or the failure to exercise or perform a discretionary function or duty on the part of a federal agency or an employee of the Government, whether or not the discretion involved be abused.” *Id.*

²⁰⁹ *Boyle v. United Techs., Corp.*, 487 U.S. 500 (1988). The Court set out the test as:

Liability for design defects in military equipment cannot be imposed, pursuant to state law, when (1) the United States approved reasonably precise specifications; (2) the equipment conformed to those specifications; and (3) the supplier warned the United States about the dangers in the use of the equipment that were known to the supplier but not to the United States.

Id. at 512. However, before applying this test, the following two elements must be present: “(a) a determination that the subject matter of the contract involves uniquely federal interests and (b) a significant conflict between an identifiable federal policy and the operation of state law.” *Dover & McGovern*, *supra* note 202, at 10. If the test is satisfied, a contractor is eligible for a qualified immunity:

[T]he defense does not protect the manufacturer of a product ordered by the Government from the manufacturer's stock. Moreover, it is not enough for the contractor to prove that it acted in accordance with the Government's direction. It must also establish that allowing the plaintiff to challenge the contractor's actions under state law would be inconsistent with a specific and significant exercise of Federal Government discretion.

Id. (citing *Boyle*, 487 U.S. at 511). A rationale offered for this exception is that it “prevents courts from second-guessing legislative and administrative conduct that implements policy goals.” Andrew Finkelman, *Suing the Hired Guns: An Analysis of*

Contractor Defense (GCD), is frequently raised by defense contractors when an alleged tort occurs inside the United States.²¹⁰

The second prominent contractor defense consists of an alternative version of the GCD, one based instead on the FTCA's combatant activities exception.²¹¹ This defense was adopted by the United States Court of Appeals for the Ninth Circuit in *Koohi v. United States*.²¹² The *Koohi* court extended the protections of the GCD to weapon manufacturers sued for harm caused to a perceived enemy by the U.S. military using such weapons.²¹³ In *Bentzlin v. Hughes Aircraft Company*, the *Koohi* holding was expanded by a federal district court to

Two Federal Defenses to Tort Lawsuits Against Military Contractors, 34 BROOK. J. INT'L L. 395, 397 (2009) (citing *United States v. S.A. Empresa de Viacao Aerea Rio Grandense*, 467 U.S. 797, 814 (1984)).

²¹⁰ Jeremy Joseph, *Striking the Balance: Domestic Civil Tort Liability for Private Security Contractors*, 5 GEO. J.L. & PUB. POL'Y 691, 712 (2007) ("[Private security contractors] sued under state tort law principles are almost uniformly invoking the GCD.").

²¹¹ 28 U.S.C. § 2680(j) (2006). Excepted from the Government's consent to suit is "any claim arising out of the combatant activities of the military or naval forces, or the Coast Guard, during time of war." *Id.* One rationale offered for this exception is "it being the nature of the sovereign at war to be able to incur injury and death without tort liability." Mateo Taussig-Rubbo, *Outsourcing Sacrifice: The Labor of Private Military Contractors*, 21 YALE J.L. & HUMAN. 101, 141 (2009). Another rationale offered for this exception is the need to "restrict interference with decisions of federal agents regarding military affairs." Finkelman, *supra* note 209, at 405 (citing *Johnson v. United States*, 170 F.2d 767, 769 (9th Cir. 1948)). The FTCA also prohibits suits against the government based on intentional torts and suits involving torts arising outside the United States. *Id.* §§ 2680(h), 2680(k). However, these aspects of the FTCA have not been extended to cover the activities of Government contractors. *See, e.g., Ibrahim v. Titan Corp.*, 391 F. Supp. 2d 10, 19 n.6 (D.D.C. 2005); Valerie C. Charles, *Hired Guns and Higher Law: A Tortured Expansion of the Military Contractor Defense*, 14 CARDOZO J. INT'L & COMP. L. 593, 612–13 (2006).

²¹² 976 F.2d 1328 (9th Cir. 1992).

²¹³ *Id.* at 1336–37 (9th Cir. 1992); *see Bentzlin v. Hughes Aircraft Co.*, 833 F. Supp. 1486, 1493 (C.D. Cal. 1993).

In *Koohi*, the Ninth Circuit recognized three principles underlying the combatant activities exception to the FTCA. These principles are based on the premise that the objectives of tort law—deterrence, punishment, and providing a remedy to innocent victims—are inconsistent with the government's interests in combat, and thus tort law cannot be applied to government actions in combat. Similarly, the application of tort law to contractors for suits arising from combat would frustrate government combat interests.

Id.

cover weapon manufacturers whose weapons injure U.S. troops in combat.²¹⁴ And in the recent GWOT case of *Ibrahim v. Titan Corp.*, a district court extended the combatant activities exception to a matter involving intentional torts, with the dispositive factor the degree of control of the military over defense contractor employees at the time the torts were committed.²¹⁵ According to the *Ibrahim* court, the combatant activities exception has application where defense contractor employees have become “soldiers in all but name.”²¹⁶ However, this exception is somewhat controversial.²¹⁷

Some district courts elected not to follow the Ninth Circuit’s lead regarding the combatant activities exception, particularly in cases that do

²¹⁴ See *Bentzlin*, 833 F. Supp. at 1494 (“[A] government contractor who manufactures [sic] the weapons of war cannot be held liable for deaths of American soldiers arising from combat activity.”).

²¹⁵ *Ibrahim v. Titan Corp.*, 556 F. Supp. 2d 1, 5 (D.D.C. 2007).

Where contract employees are under the direct command and exclusive operational control of the military chain of command such that they are functionally serving as soldiers, preemption ensures that they need not weigh the consequences of obeying military orders against the possibility of exposure to state law liability. It is the military chain of command that the FTCA’s combatant activities exception serves to safeguard, however, and common law claims against private contractors will be preempted only to the extent necessary to insulate *military* decisions from state law regulation. This is why the degree of operational control exercised by the military over contract employees is dispositive.

Id.

²¹⁶ *Ibrahim*, 391 F. Supp. 2d at 18.

²¹⁷ See *Carmichael v. Kellogg Brown & Root Servs., Inc.*, 450 F. Supp. 2d 1373, 1379 (N.D. Ga. 2006).

Just one paragraph of the court’s opinion in *Koohi* is devoted to the issue of whether the plaintiffs’ claim against the defense contractors was preempted in accordance with *Boyle*. And that one paragraph is conclusory, not analytical.

....

Finally, *Koohi* represents an expansion of the holding in *Boyle* that the Supreme Court may or may not have intended.

Id.

not involve manufacturing or design defects.²¹⁸ With this exception currently in flux,²¹⁹ defendant defense contractors who might otherwise qualify for the protection may not be granted relief. Despite the district courts' reluctance to expand the defense, some commentators have recently urged its expansion to include even more combat zone situations.²²⁰ With such divergent opinions on the combatant activities exception rampant, this exception is ripe for Supreme Court resolution.

²¹⁸ See generally *McMahon v. Presidential Airways, Inc.*, 460 F. Supp. 2d 1315 (M.D. Fla. 2006), *aff'd*, 502 F.3d 1331 (11th Cir. 2007); *Carmichael*, 450 F. Supp. 2d 1373; *Lessin v. Kellogg Brown & Root*, No. H-05-01853, 2006 U.S. Dist. LEXIS 39403 (S.D. Tex. Jun. 12, 2006). *Koohi* and *Bentzlin* were followed by a product liability case involving the alleged defective manufacture of a helmet (and its component parts) worn by a helicopter pilot. *Flanigan v. Westwind Techs., Inc.*, No. 07-1124, 2008 U.S. Dist. LEXIS 82203 (W.D. Tenn. Sept. 15, 2008). *Flanigan* acknowledged the differences between convoy service cases and cases involving "complex equipment acquired by the Government in its procurement process, which inevitably implicates nuanced discretion and sophisticated judgments by military experts." *Id.* at *35-36 (quoting *Carmichael*, 450 F. Supp. 2d at 1380-81). Another district court has framed the test for application of the combatant activities exception as a question of whether the plaintiff's claim arises from "active military combat operations." *Harris v. Kellogg, Brown & Root Servs., Inc.*, No. 08-563, 2009 U.S. Dist. LEXIS 26547, at *92-93 (W.D. Pa. Mar. 31, 2009).

²¹⁹ See generally *Joseph*, *supra* note 210, at 693 ("[T]he civil tort liability regime applicable to [private security contractor] operations in war zones appears to lack uniform standards and predictable treatment.").

²²⁰ See Aaron L. Jackson, *Civilian Soldiers: Expanding the Government Contractor Defense to Reflect the New Corporate Role in Warfare*, 63 A.F. L. REV. 211, 221 (2009); Trevor Wilson, *Operation Contractor Shield: Extending the Government Contractor Defense in Recognition of Modern Wartime Realities*, 83 TUL. L. REV. 255, 280 (2008) (calling for "an extension of the GCD to shield [private military contractors] when[ever] they take up arms on the battlefield with the U.S. military"); see also John L. Watts, *Differences Without Distinctions: Boyle's Government Contractor Defense Fails to Recognize the Critical Differences Between Civilian and Military Plaintiffs and Between Military and Non-Military Procurement*, 60 OKLA. L. REV. 647, 675 (2007) (calling for a new "military contractor defense" that "would not apply to claims brought by civilian plaintiffs but would bar all products liability claims brought by servicemembers injured incident to service . . ."); *Joseph*, *supra* note 210, at 717 (referring to courts' refusal to extend *Boyle's* holding to service contracts as "narrowly constrained" and "strange"). Because most contractors engaged in GWOT support provide services rather than the manufacture of goods, these two FTCA exceptions have proven thus far to be of limited use. *Finkelman*, *supra* note 209, at 397 (citing Sam Perlo-Freeman & Elisabeth Sköns, *The Private Military Services Industry*, SIPRI INSIGHTS ON PEACE AND SECURITY 8 (2008)); *Jackson*, *supra* note 220, at 212.

Arising from the doctrine of sovereign immunity, the GCD provides absolute immunity to contractors facing negligence, warranty, or strict liability claims due to incidents caused by defective designs. But what protection is currently provided to contractors employed by

Another possible course of action for defense contractors performing contingency contracts is to seek indemnification from the Government for tort damages awards.²²¹ The Anti-Deficiency Act²²² generally prohibits the use of indemnification agreements in Government contracts,²²³ but there are a few exceptions.²²⁴ One that could most likely provide relief to defense contractors in war zones is found under Public Law 85-804.²²⁵ This exception “provid[es] compensation to the contractor in the event of liability to third parties incurred while performing contractual duties involving ‘unusually hazardous’ risks.”²²⁶ If such an indemnification request is approved, the contract will include Federal Acquisition Regulation (FAR) clause 52.250-1, *Indemnification Under Public Law 85-804*, which provides indemnification for third-party tort claims resulting from the unusually hazardous risk specified in

the government to perform service-based contracts? Simply put, nothing.

Id.

²²¹ Dover & McGovern, *supra* note 202, at 1 (“In commercial contracting, contractual indemnification is an important risk mitigation tool.”).

²²² The Anti-Deficiency Act is

[a] statute prohibiting Government agencies from obligating the Government, by contract or otherwise, in excess of or in advance of appropriations, unless authorized by some specific statute. Codified at 31 U.S.C. § 1341 et seq. since 1982, the Act prevents Government employees from involving the government in expenditures or liabilities beyond those contemplated and authorized by Congress.

NASH, JR. ET AL., *supra* note 134, at 30.

²²³ Dover & McGovern, *supra* note 202, at 1.

²²⁴ *Id.* at 2–4 (citing as potential options: Pub. L. No. 85-804, 72 Stat. 972 (1958); the Price-Anderson Act, 42 U.S.C. §§ 2210 (1994); indemnification for research and development contractors under 10 U.S.C. § 2354 (2006); GENERAL SERVS. ADMIN. ET AL., FEDERAL ACQUISITION REG. pt. 52.228-7 (Jan. 2009) [hereinafter FAR]).

²²⁵ Dover & McGovern, *supra* note 202, at 2 (“P.L. 85-804 [] is an exception to the general rule providing that the Government may not enter into open-ended indemnification agreements.”).

²²⁶ C. Douglas Goins, Jr. et al., *Regulating Contractors in War Zones: A Preemptive Strike on Problems in Government Contracts*, (07-3 Briefing Papers) 22 (Thomson & West 2007).

the contract.²²⁷ However, the high-level approval requirement²²⁸ of this FAR clause limits its practical use.²²⁹

Another source in the FAR for potential indemnification of contractors in contingency environments is FAR 52-228.7, *Insurance—Liability to Third Persons*.²³⁰ Under this clause, indemnification for third party liability becomes available for costs not otherwise provided for, but only in cost reimbursement type contracts.²³¹ Fixed price contracts are not included under this clause.²³² Unlike indemnification under Public Law 85-804, indemnification under FAR 52.228-7 is “subject to the availability of appropriated funds at the time a contingency occurs.”²³³ If the high-level approval requirement and fund availability issues can be overcome, indemnification could serve as a viable option for defense contractors seeking to recover funds paid out pursuant to tort damages awards.

Another potential avenue of relief for combat zone defense contractors is the Defense Base Act (DBA).²³⁴ The DBA provides for worker’s compensation insurance for certain types of employment taking place outside the United States.²³⁵ If applicable, the DBA serves as the

²²⁷ Dover & McGovern, *supra* note 202, at 2.

²²⁸ FAR, *supra* note 224, pt. 50.201(d). Permission for such indemnification “shall be exercised only by the Secretary or Administrator of the Agency concerned” *Id.*

²²⁹ Furthermore, indemnification under Public Law 85-804 is described by defense contractor advocates as “burdensome,” “unpredictable,” and “not consistently applied.” Goins, *supra* note 226, at 22 n.219 (quoting *Iraq Reconstruction: Hearing Before the H. Comm. On Oversight and Government Reform*, 110th Cong. 8 (2007) (statement of Alan Chvotkin, Senior Vice President and Counsel, Prof’l Servs. Council)).

²³⁰ FAR, *supra* note 224, pt. 52-228.7; U.S. DEP’T OF DEFENSE, DEFENSE FEDERAL ACQUISITION REG. SUPP. pt. 228.311-1 (Jan. 1, 2009) [hereinafter DFARS] (directing that the FAR clause be included).

²³¹ FAR, *supra* note 224, pt. 28.311-1; Goins, *supra* note 226, at 22; Joseph, *supra* note 210, at 706. The American Bar Association’s Section of Public Contract Law has expressed a desire for this clause to be endorsed for use in fixed price contracts as well as cost reimbursement contracts. Goins, *supra* note 226, at 22 n.221 (citing Letter from Robert L. Schaefer, Chair, Section of Public Contract Law, to Dean G. Propps, Principal Deputy to the Assistant Secretary of the Army (Oct. 12, 2005), available at http://www.abanet.org/contract/federal/regscmm/emerging_007.pdf).

²³² Goins, *supra* note 226, at 22.

²³³ FAR, *supra* note 224, pt. 52.228-7(d); Dover & McGovern, *supra* note 202, at 4.

²³⁴ 42 U.S.C. §§ 1651–54 (2006).

²³⁵ *Id.* § 1651(a)(1)-(2); *Nordan v. Blackwater Sec. Consulting, LLC*, 382 F. Supp. 2d 801, 807 (4th Cir. 2005) (“The DBA is a federal statute that incorporates and extends the comprehensive worker’s compensation scheme established by the Longshore and Harbor Worker’s Compensation Act (LHWCA) to select forms of employment outside of the

exclusive remedy against defense contractors for injuries sustained on the job by defense contractor personnel.²³⁶ Employer liability under the DBA limits itself to “medical and disability benefits, statutory death benefits, payment for reasonable funeral expenses, and compensation payments to surviving eligible dependents.”²³⁷ However, disagreement currently exists among the federal courts as to the DBA’s applicability.²³⁸ The United States Court of Appeals for the Fourth Circuit held the DBA did not preempt state tort law claims because the DBA’s statutory scheme did not specifically provide for a federal cause of action.²³⁹ However, other courts have found preemption to be warranted under the DBA.²⁴⁰ Recent congressional frustration with the DBA’s administration²⁴¹ may ultimately bring changes that resolve these judicial disagreements via statute. Otherwise, the DBA is another area ripe for Supreme Court resolution.

Having addressed the GWOT developments in the political question doctrine and other relevant judicially-recognized limits on defense contractor tort liability, the focus now shifts to the effect these measures will have on Government contingency contracting.

United States.”) (citation omitted). Types of employment covered under the DBA (via the LHWCA) consist of the

injury or death of any employee engaged in any employment—at any military, air, or naval base acquired after January 1, 1940, by the United States from any foreign government; or upon any lands occupied or used by the United States for military or naval purposes in any Territory or possession outside the continental United States.

42 U.S.C. § 1651(a)(1)-(2).

²³⁶ 33 U.S.C. § 904 (2006); *Nordan*, 382 F. Supp. 2d at 808; Dover & McGovern, *supra* note 202, at 9 (“If an injured worker is covered under the DBA, the worker is generally entitled to the benefits and procedures set forth in the [LHWCA]. The LHWCA is supposed to provide the exclusive remedy against a qualifying employer for injury or death of the employee.”) (footnote omitted).

²³⁷ Dover & McGovern, *supra* note 202, at 9.

²³⁸ See *infra* notes 239–40 and accompanying text.

²³⁹ *Nordan*, 382 F. Supp. 2d at 809–11.

²⁴⁰ See, e.g., *Nauert v. Ace. Prop. & Cas. Ins. Co.*, No. 04-CV-02547-WYD-BNB, 2005 U.S. Dist. LEXIS 34497 (D. Colo. Aug. 27, 2005); *Ross v. Dyncorp*, 362 F. Supp. 2d 344 (D.D.C. 2005); *Schmidt v. Northrop Grumman Sys., Corp.*, No. 3:04-CV-042-JTC, 2005 U.S. Dist. LEXIS 24688 (N.D. Ga. Mar. 2, 2005).

²⁴¹ See generally 50 GOVERNMENT CONTRACTOR ¶ 191 (2008). In testimony before the House Oversight and Government Reform Committee on 15 May 2008, the Committee “expressed frustration with apparent waste and mismanagement” of DBA insurance programs. *Id.*

VIII. Impact on Government Contingency Contracting

Judges and scholars openly speculate about the possible consequences of defense contractor tort liability on the federal procurement process. In *Boyle*, the Supreme Court warned that “[t]he financial burden of judgments against [] contractors would ultimately be passed through, substantially if not totally, to the United States itself, since defense contractors will predictably raise their prices to cover, or to insure against, contingent liability”²⁴² The *Nash & Cibinic Report* cited earlier alerted to “significant risks” to contractors due to the recent developments in the political question doctrine and intimated contractors may lose their desire to perform such contracts in the future.²⁴³ But is the situation really this dire? Are contractors at a point where, because of increased litigation risks, they will be forced to charge the Government more for their services or elect to not provide services altogether?

The answers may not be far away. In November 2008, Joshua Eller filed suit in the U.S. District Court for the Southern District of Texas, as a result of injuries he suffered at Balad Air Base, Iraq, while deployed as a contractor employee of KBR from February to November of 2006.²⁴⁴ The complaint alleges defendants KBR and Halliburton “intentionally and negligently exposed thousands of soldiers, contract employees and other persons to unsafe water, unsafe food, and contamination due to faulty waste disposal systems”²⁴⁵ The complaint also includes allegations of injury from toxic smoke which emanated from an open air burn pit at Balad.²⁴⁶ The complaint alleges approximately 1,000 other individuals suffered similar injuries and it seeks to combine all of those actions into a single class action lawsuit.²⁴⁷ More significantly, this

²⁴² *Boyle v. United Techs., Corp.*, 487 U.S. 500, 511–12 (1988). The same point was made in the *Ibrahim* case. *Ibrahim v. Titan Corp.*, 391 F. Supp. 2d 10, 18 (D.D.C. 2005) (“[T]he government will eventually end up paying for increased liability through higher contracting prices (or through an inability to find contractors willing to take on certain tasks)”).

²⁴³ See *supra* note 5.

²⁴⁴ Complaint at 1–2, *Eller v. Kellogg Brown & Root*, No. 4:2008cv03495 (S.D. Tex. Nov. 28, 2008); see Kennedy, *supra* note 95, at 31.

²⁴⁵ Complaint, *supra* note 244, at 1.

²⁴⁶ *Id.* at 9–10; see Adam Levine, *Effects of Toxic Smoke Worry Troops Returning From Iraq*, CNN.com, Dec. 15, 2008, <http://www.cnn.com/2008/12/15/burn.pits/index.html>.

²⁴⁷ Complaint, *supra* note 244, at 2–4.

action is only one of several suits currently pending that relate to similar KBR activities in Iraq.²⁴⁸

The political question doctrine will be a major factor in this coming storm of litigation. With the large number of potential plaintiffs compounded by the seriousness of the conduct and injuries alleged, these suits have the potential to dwarf the damages awards previously sought in earlier GWOT cases. Undoubtedly, KBR will seek to raise the political question doctrine as an absolute bar to these and any similar suits.²⁴⁹ Thanks to *McMahon, Lane*, and the other GWOT political question cases, federal district courts now have a workable political question framework in place to navigate from. The question then becomes how this coming storm will impact Government contingency contracting.

Defense contractor advocates warn of “deleterious effects” to the mission and the contractor–military relationship if tort suits against war zone defense contractors are allowed to proceed.²⁵⁰ They argue such tort claims “frustrate” and “conflict with” the Government’s ability to control contingency operations and would result in compromised logistical support and mission jeopardy.²⁵¹ Furthermore, many companies, especially smaller ones, could be deterred from seeking contingency contracts.²⁵² For those contractors who do elect to proceed, they will seek to insulate themselves from liability by either self-insuring or obtaining insurance coverage, if it is available.²⁵³ The argument continues that such costs will then be passed onto the Government in the form of higher contract prices.²⁵⁴ But, most alarmingly, some defense

²⁴⁸ See Kelly Kennedy, *5 More Burn-Pit Lawsuits Filed Against KBR*, AIRFORCETIMES.COM, June 16, 2009, http://airforcetimes.com/news/2009/06/military_burnpit_lawsuits_061609w/; Kelly Kennedy, *KBR Sued Over Burn-Pit Exposure*, ARMY TIMES, May 11, 2009, at 13; Scott Bronstein & Abbie Boudreau, *Guardsmen Sue KBR Over Chemical Exposure*, CNN.COM, Dec. 3, 2008, <http://www.cnn.com/2008/US/12/03/guardsmen.toxic/index.html>.

²⁴⁹ See generally *supra* notes 86, 88–171, and accompanying text.

²⁵⁰ Prof’l Servs. Council Amicus Brief, *supra* note 11, at *10, *13. See generally Brief for Nat’l Def. Indus. Ass’n as Amicus Curiae Supporting Appellees at *10, *23, *Lane v. Halliburton*, No. 06-20874 (S.D. Tex. 2006).

²⁵¹ Brief Prof’l Servs. Council Amicus Brief, *supra* note 11, at *13, *46.

²⁵² *Id.* at *46.

²⁵³ *Id.*; Goins, *supra* note 226, at 22 (“The most rational behavior on the part of contractors may be to insure themselves against potential liabilities because the extent of liability to a potential claimant can be too great for self-insurance.”).

²⁵⁴ See *supra* note 242 and accompanying text.

contractor advocates claim the impact of such suits “would be far more profound than financial” and defense contractors may, out of a fear of being sued, refuse to follow the military’s instructions altogether.²⁵⁵

Unlike the voices heard by Horton, which actually existed, the consequences predicted by defense contractor advocates vastly overstate the actual impact these GWOT tort suits will have on Government contingency contracting. Several reasons exist for this contention. First, the Government currently pays far too much money to defense contractors overseas for them to now decline performance of contingency contracts.²⁵⁶ The alleged dramatic price increases in U.S. Government contracts due to the increased litigation risk are unlikely as well.²⁵⁷ Contract prices may rise to some degree, but the Government can ill afford to refuse to pay them.²⁵⁸ Second, the U.S. military does not

²⁵⁵ *Supra* note 11.

²⁵⁶ See *supra* note 83 and accompanying text; Michael Hurst, Essay, *After Blackwater: A Mission-Focused Jurisdictional Regime for Private Military Contractors During Contingency Operations*, 76 GEO. WASH. L. REV. 1308, 1325 n.104 (2008) (“Since September 2001, the Congress has appropriated \$602 billion for military operations and other activities related to Iraq, Afghanistan, and the war on terrorism.”) (quoting *Estimated Costs of U.S. Operations in Iraq and Afghanistan and of Other Activities Related to the War on Terrorism: Hearing Before the H. Comm. on the Budget*, 110th Cong. (2007) (statement of Robert A. Sunshine, Assistant Director for Budget Analysis, Congressional Budget Office), available at http://www.cbo.gov/ftpdocs/84xx/doc8497/07-30-WarCosts_Testimony.pdf). To further place the U.S. Government’s financial investment in GWOT contingency contracting into context, the \$20 billion contract awarded to KBR for logistics operations in Iraq was “roughly three times the total amount America spent to win the first Gulf War.” Major Jeffrey S. Thurnher, *Drowning in Blackwater: How Weak Accountability over Private Sector Contractors Significantly Undermines Counterinsurgency Efforts*, ARMY LAW., July 2008, at 64, 68 (citing P.W. Singer, *Can’t Win with ‘Em, Can’t Go to War Without ‘Em: Private Military Contractors and Counterinsurgency*, FOR. POL’Y AT BROOKINGS 10 (Policy Paper No. 4) (2007), available at <http://www.brookings.edu/~media/Files/rc/papers/2007/0927militarycontractors/0927militarycontractors.pdf>).

²⁵⁷ Hurst, *supra* note 256, at 1325 n.103 (“Given the large number of firms in the industry and the competitive nature of the bidding process, it is unlikely that firms would be able to demand dramatic price increases.”).

²⁵⁸ See e-mail from Paul M. McQuain, Director, DCMA Lockheed Martin Ft. Worth, to author (Feb. 28, 2009) (on file with author). Mr. McQuain is a retired U.S. Army colonel and previously served in a contingency environment as the DCMA Commander for Iraq. He believes such tort suits against contractors, if allowed to proceed, would cause contracting costs to increase, but that they would not “have a significant impact on DoD’s ability to find contractors to bid on contracts such as LOGCAP.” *Id.*; see also Telephone Interview with Daryl Conklin, Deputy Director, DCMA Special Programs South, in Charlottesville, Va. (Feb. 27, 2009). Mr. Conklin is a retired U.S. Army lieutenant colonel and previously served in contingency environments as the DCMA Deputy Commander for Iraq and the Chief of Contracting for U.S. Forces in Croatia. He believes

own the internal means to provide the goods and perform the services contracted for in a contingency environment—such goods and services are necessary for mission accomplishment.²⁵⁹ Finally, as discussed earlier, apart from the political question doctrine, defense contractors who face allegations of tortious conduct in a contingency environment have several legal defenses and other alternatives to limit or avoid liability, including insurance.²⁶⁰ Viewed together, these points counter forecasts of the impending ruin of Government contingency contracting.

With their recent activity involving the political question doctrine, courts have hardly thrust open the floodgates to litigation. Rather, they have properly focused their attention on protecting military decision-making and policy from judicial intrusion, and limited their rulings accordingly. For those suits that do not question military decisions or policy, they will move forward (at least without political question problems). This may or may not cause an increase in contractor costs

the government will cover any associated cost increases in order to facilitate mission accomplishment. *Id.*

²⁵⁹ Conklin, *supra* note 258. According to Mr. Conklin, the U.S. military does not have the capability to perform contingency contracting services itself because it previously eliminated most of those functions when it “cut off its logistical tail” in the 1990s. *Id.* As such, the military no longer employs the organic forces necessary to provide sufficient LOGCAP-type services and personal protective services which make up a large part of Government contingency contracts. *Id.*; see GAO REP., *supra* note 83, at 1. See generally JACQUES S. GANSLER ET AL., URGENT REFORM REQUIRED: ARMY EXPEDITIONARY CONTRACTING, REPORT OF THE “COMMISSION ON ARMY ACQUISITION AND PROGRAM MANAGEMENT IN EXPEDITIONARY OPERATIONS” (2007) (discussing the consequences of cutbacks in Army contracting operations beginning in 1991). The GAO found the vast number of GWOT contracts and contractor employees represents “an increased reliance on contractors to carry out agency missions.” GAO REP., *supra* note 83, at 1. Such personnel perform duties ranging from “interpretation/translation, security, weapons system maintenance, intelligence analysis, facility operations support, [to] road construction.” *Id.* See generally Addicott, *supra* note 7, at 346–47 (attributing the increased reliance on combat zone defense contractors to several factors).

First, Congressional limits on the number of DOD personnel extend both to the size of the armed forces in general and to the number of uniformed personnel authorized in a particular operational mission or area. Second, the ever-increasing sophistication and automation of a wide variety of technologies used by the military requires a workforce that often is not found in the uniformed services. Finally, strategic and tactical needs mandate that the command authority conserve DOD resources to address unanticipated exigencies.

Id. (footnote omitted).

²⁶⁰ *Supra* Section VII; see *supra* note 253 and accompanying text.

due to higher insurance premiums related to tort damages, which could then be conveyed to the U.S. Government in the form of higher prices. However, the political question doctrine's purpose is *not* to inhibit the principles of accountability²⁶¹ inherent in the American tort law system. For those who wish to change this system, they should look instead toward the political branches or state governments for relief. These entities have in their arsenals statutes, regulations, and other mechanisms more appropriate for change. Such methods are much more apt for this purpose than reliance on a mutation of the political question doctrine into a form beyond its established limits.

To argue that Government contingency contracting will break down unless the political question doctrine extends to all tort suits brought against combat zone defense contractors is disingenuous. Alarming predictions of compromised logistics and mission failure grossly exaggerate the effect of these GWOT tort suits on combat zone contractors and Government contingency contracting. Such hyperbole ignores the reality and degree of the U.S. Government's financial commitment to and dependency on contingency contracting in Iraq and Afghanistan. Finally, even if the consequences to the DoD procurement system are as dire as defense contractor advocates have alleged, the political branches are in a much more appropriate position to remedy them and can do so much more immediately and effectively.

*That one small, extra Yopp put it over!
Finally, at last! From that speck on that clover
Their voices were heard! They rang out clear and clean.*

²⁶¹ See generally Jason M. Solomon, *Equal Accountability Through Tort Law*, 103 NW. U. L. REV. (forthcoming 2009). The purpose of tort law is to "provid[e] a vehicle for individuals to bring about justice, and in doing so, [to] vindicate[e] the notion of a community of equals who are answerable to one another, and expected to treat one another with equal respect." *Id.*; MCQUILLAN & ABRAMYAN, *supra* note 8, at 1.

An efficient tort system is an important part of a thriving free-enterprise economy. It ensures that firms have proper incentives to produce safe products in a safe environment, and that truly injured people are fully compensated. An efficient tort system results in greater trust among market participants, leading to more trading, and eventually a higher standard of living for individuals in the society. An efficient tort system benefits all.

Id.

*And the elephant smiled. "Do you see what I mean?"*²⁶²

IX. Conclusion

The political question doctrine is an established, important part of the American judicial system. It protects the separation of powers by restricting courts from adjudicating matters better left to other branches of Government. Recently, federal courts have applied the doctrine to cases involving allegations of tortious conduct on the part of defense contractors engaged in GWOT support. In their analysis, courts have cautiously avoided passing judgment on executive policy and military decision-making. Cases that required such action were found to present political questions and were dismissed. Alternatively, cases that only required the courts to apply well-settled tort law standards were allowed to proceed. With more serious litigation on the horizon, courts now have a reliable framework to employ. Some defense contractor advocates have predicted dire consequences for the Government's contingency contracting process if tort cases against combat zone defense contractors are allowed to proceed. However, the nature and degree of the Government's commitment to contingency contracting indicates otherwise. The bottom line is that tort suits against defense contractors that are not terminated as political questions *will* have an effect on contingency contracting—but the severity of that impact has been *far* overstated by defense contractor advocates.

Ultimately, Horton's success in winning over the Jungle of Nool came from the fact that the Whos were real—not imagined. Defense contractor predictions of impending doom are quite the opposite. Recent political question doctrine developments will not alter the nature of Government contingency contracting. Halliburton does not hear a Who.

²⁶² SEUSS, *supra* note 1, at 58.

**CAPITALIZING “F” IS NOT ENOUGH: THE ARMY SHOULD
REVISE ITS POSTPARTUM LEAVE POLICIES TO BETTER
SUPPORT THE ARMY FAMILY**

MAJOR SARA M. ROOT*

*To further acknowledge the role Army spouses and
children of Soldiers play in today’s military, the director
of the Army staff has instructed for the word Families to
be capitalized in all official correspondence.¹
We are committed to providing our Families a strong,
supportive environment where they can thrive.²*

* Judge Advocate, U.S. Army. Presently assigned as Branch Chief, Government Appellate Division, Arlington, Va. LL.M., 2009, The Judge Advocate Gen.’s Legal Ctr. & Sch., U.S. Army, Charlottesville, Va.; J.D., 2006, Campbell University, N.C.; B.A., 1997, Norwich University, Vt. Previous assignments include Chief, Rule of Law, XVIII Airborne Corps, Multi-National Corps–Iraq, Baghdad, Iraq, 2008; Trial Counsel and Senior Trial Counsel, XVIII Airborne Corps, Fort Bragg, N.C., 2007–2008, Assistant Brigade S2, 325th Airborne Infantry Regiment, 82d Airborne Division, Fort Bragg, N.C., 2001–2002, Deputy G2 Plans Officer, Fort Campbell, Ky., 2000–2001; G2 Plans Officer, 10th Mountain Division, Tuzla, Bosnia, 2000; Battalion S2 Officer, 326th Combat Engineer Battalion, 101st Airborne Division (Air Assault), Fort Campbell, Ky., 1999–2000, Platoon Leader, 311th Military Intelligence Battalion, 101st Airborne Division (Air Assault), Fort Campbell, Ky., 1997–1999. Member of the North Carolina Bar. This article was submitted in partial completion of the Master of Laws requirements of the 57th Judge Advocate Officer Graduate Course. The author would like to thank her family (especially her three children), and Lieutenant Colonel Suzy Mitchem for her support and advice in writing this article.

¹ IMCOM, Europe—Public Affairs, *Uppercasing ‘Families’ Highlights Support*, ARMY.MIL NEWS, Apr. 24, 2007, <http://www.army.mil/-news/2007/04/24/2831-uppercasing-families-highlights-support/>; E-mail from Lieutenant General James L. Campbell, Director of the Army Staff, to General John Abizaid et al. (Apr. 18, 2007, 09:46 EST) (on file with author) (instructing commanders to widely disseminate the Acting Secretary of the Army’s and the Chief of Staff of the Army’s guidance on capitalizing the word “family” when used to describe U.S. military families).

² *Army Family Covenant*, <http://www.army.mil/-images/2007/10/10/9140/army.mil-2007-10-10-164403.jpg> (last visited Mar. 9, 2009) [hereinafter *Army Family Covenant*] (showing the Army Family Covenant signed 17 October 2007 by Secretary of the Army Peter Geren, Chief of Staff of the Army General W. Casey, Jr., and Sergeant Major of the Army Kenneth O. Preston in recognition of Army families); Elizabeth M. Lorge, *Army Leaders Sign Covenant with Families*, ARMY.MIL NEWS, Oct. 17, 2007, <http://www.army.mil/-news/2007/10/17/5641-army-leaders-sign-covenant-with-families/> (“The Army wants to provide Soldiers and their Families with a level of support commensurate with their level of service, and the covenant is in direct response to concerns from Army Families.”) (quoting General W. Casey Jr.).

I. Introduction

The eight-week-old infant developed a 104-degree temperature. A few hours later, the mother rushed the baby to the emergency room. The infant's fever was rising, even with medication. A doctor examined the baby and immediately called the neonatal specialist. Within moments, the doctors inserted a catheter and tube into the baby's spinal cord and turned the baby over. The mother watched in horror as the fluid drained from her baby's spinal cord. The diagnosis: meningitis. The baby would have died before the day was over had he not been treated. The source of the meningitis: exposure to bacteria carried by an older infant in the same daycare center. The difference in age between the two infants: seven months. The older infant was nine months old and therefore, had a more developed immune system to fight the bacteria. The eight-week-old infant's less established immune system could not defeat the nearly fatal bacteria on its own. The doctor told the mother that children three months and younger should not be in childcare centers because of the substantially increased risk of illness.³

In this situation, the mother did not have the option to be home for three months. She was an active component servicemember,⁴ and the Army authorizes only six weeks of convalescent leave for a mother after childbirth. Originally, her commander granted an additional two weeks of ordinary leave. However, the mother's supervisor needed her in the office, and he revoked her additional leave. If the Family and Medical Leave Act⁵ (FMLA), which applies to civilians, applied to this active component mother, her infant would not have had to be in a daycare center and would not have contracted meningitis from the other child. The time has come for Congress to expand military leave entitlements⁶ to include provisions similar to those provided by the FMLA.

³ In order to protect the privacy of the minor child, the name of the servicemember is not included.

⁴ "Active component" refers to servicemembers serving an active duty service obligation. "Active duty" includes active component and can also refer to activated U.S. Army Reserve and National Guard servicemembers. Because retention issues and policies vary between U.S. Army Reserve, National Guard, and active component personnel, the author focuses on the active component throughout the article for purposes of consistency. *See infra* Section V.

⁵ Family and Medical Leave Act of 1993, 29 U.S.C. §§ 2601–2654 (2006).

⁶ 10 U.S.C. § 701 (2006).

During legislative hearings from 1985 to 1993, the United States (U.S.) Congress considered hundreds of other situations similar to the example above in attempting to establish a national family leave policy.⁷ Each example involved the almost impossible choice between family and financial security by virtue of sustained employment.⁸ Congress also heard counter-arguments from business owners describing the hardships they would face by being forced to implement the proposed labor protections.⁹ Finally, in 1993, President William J. Clinton signed Public Law 103-3, the FMLA.¹⁰ The FMLA provides up to twelve weeks of unpaid leave for “eligible employees”¹¹ under certain qualifying conditions.¹² Active duty servicemembers are not eligible employees.¹³

⁷ See, e.g., *Parental and Disability Leave: Joint Hearing on H.R. 2020 Before the Subcomm. on Civil Serv. and the Subcomm. on Compensation & Employee Benefits of the Comm. on Post Office & Civil Serv., and the Subcomm. on Labor Mgmt. Relations & the Subcomm. on Labor Standards of the Comm. on Educ. & Labor*, 99th Cong. 21 (1985) [hereinafter *PDLA H.R. Hearing*] (statement of Liberia Johnson, Parent, Charleston, S.C.); *Family and Medical Leave Act of 1993: Hearing on S. 5 Before the Subcomm. on Children, Family, Drugs, & Alcoholism of the Comm. on Labor & Human Resources*, 103d Cong. 21–24 (1993) (statements of Linda & Rudy Fernandez, Parents, Lynn, Mass.). In addition to these hearings, twelve other hearings took place during that time frame.

⁸ See sources cited *supra* note 7.

⁹ See, e.g., *Parental and Medical Leave Act of 1986: Joint Hearing on H.R. 4300 Before the Subcomm. on Labor-Management Relations and the Subcomm. on Labor Standards of the Comm. on Educ. & Labor*, 99th Cong. 79 (1986) (statement of Barbara Inkellis, General Counsel of Disclosure Information Group); *Family and Medical Leave Act of 1993: Hearing on H.R. 1 Before the Subcomm. on Labor-Mgmt. Relations of the Comm. on Educ. & Labor*, 103rd Cong. 91–101 (1993) (prepared statement of the National Federation of Independent Business). In addition to these hearings, twelve other hearings took place during that time frame.

¹⁰ 29 U.S.C. §§ 2601–2654.

¹¹ *Id.* § 2611(2)(A) (defining an eligible employee as an employee who had been employed for at least twelve months by the employer providing leave and “for at least 1250 hours of service with such employer during the previous twelve-month period”).

¹² *Id.* § 2612(a)(1)(A)–(D) (qualifying conditions include the birth of a son or daughter, adoption of a son or daughter, “[t]o care for the spouse, or a son, daughter, or parent, of the employee, if such spouse, son, daughter or parent has a serious health condition,” or “[b]ecause of a serious health condition that makes employee unable to perform the functions of the position of such employee”).

¹³ *Id.* § 2611(4)(A)(i) (defining eligible employee as one employed by “any person engaged in commerce or in any industry affecting commerce”). The FMLA specifically amends 5 U.S.C. § 6301 (2006) to cover civil service employees but does not amend 10 U.S.C. § 701 to cover servicemembers.

Leave authority for active duty servicemembers is provided by law and covered primarily by regulation.¹⁴ Army Regulation 600-8-10, *Leaves and Passes*, covers leave and pass programs for members of the U.S. Army.¹⁵ “Soldiers on active duty earn 30 days of leave a year with pay and allowances at the rate of 2 ½ days a month.”¹⁶ There are two different types of leave that might cover postpartum leave for an active component mother who has recently given birth: convalescent leave and ordinary leave. The Army does not have maternity leave.¹⁷

Regarding convalescent leave, hospital and unit commanders are authorized to grant up to forty-two days of convalescent leave following childbirth.¹⁸ The regulation states, “Convalescent leave is a nonchargeable absence from duty granted to expedite a soldier’s return to full duty after illness, injury, or childbirth.”¹⁹ Additionally, male and female servicemembers can request ordinary leave following the birth of a child. The unit commander has discretion in granting ordinary leave.²⁰ In addition to ordinary leave, fathers may receive paternity leave. President George W. Bush signed the National Defense Authorization Act of 2009²¹ on 14 October 2008, amending 10 U.S.C. § 701, which provides ten days paternity leave for active duty married members of the armed forces whose wife gives birth.²²

¹⁴ 10 U.S.C. § 701 (implemented in Army Regulation 600-8-10). U.S. DEP’T OF ARMY, REG. 600-8-10, LEAVES AND PASSES (15 Feb. 2006) [hereinafter AR 600-8-10]. The author mostly limits the parameters of this article to Army policies.

¹⁵ AR 600-8-10, *supra* note 14.

¹⁶ *Id.* para. 2-3.

¹⁷ The Army’s policy of providing convalescent leave is more similar to health care benefits in the civilian work force where leave is granted under temporary disability. This usually ranges from four to six weeks. Maternity leave, on the other hand, is a leave of absence for a new mother for the birth and care of her child. The Army’s policy does not provide for time to care for the baby. For example, if a servicemember mother gives birth to a premature infant that remains in the hospital for six weeks, the mother would not be entitled to any additional leave or to delay her convalescent leave to care for her infant when it is discharged from the hospital.

¹⁸ 10 U.S.C. § 70; AR 600-8-10, *supra* note 14, para. 5-3(b), (c).

¹⁹ AR 600-8-10, *supra* note 14, para. 5-3(a).

²⁰ *Id.* para. 4-3(c).

²¹ Duncan Hunter National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2009, Pub. L. No. 110-417, 122 Stat. 4356, 4449 (2008) [hereinafter NDAA 2009].

²² 10 U.S.C.S. § 701(j)(1)–(2) (LexisNexis 2008) (amended by NDAA 2009, Pub. L. No. 110-417, 122 Stat. 4356, 4449 (2008)). The Army recently issued implementing instructions. See Message, 101547Z Mar 09, PTC Washington, DC, subject: ALARACT 062/2009—Army Guidance for Paternity Leave Authorized by Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 [hereinafter Paternity Guidance].

While military regulations do provide servicemembers with options to take leave, they do not provide enough time for postpartum leave.²³ Congress could expand the FMLA to include active component servicemembers as “eligible employees.” However, applying all provisions of the FMLA to servicemembers goes too far.²⁴ This article proposes Congress amend 10 U.S.C. § 701 to entitle female servicemembers twelve weeks maternity leave following the birth of a child, male servicemembers four weeks paternity leave following the birth of a child, and male and female servicemembers six weeks parental leave following the adoption of a child.²⁵ This would provide benefits more consistent with the FMLA, state laws, international policy, and the Army’s own renewed commitment to families, without compromising the mission.²⁶

This article establishes five reasons why postpartum leave should be extended: (1) to improve infant health; (2) to improve parent health; (3) to improve infant-parent bonding; (4) to improve servicemember performance; and (5) to improve retention rates.

Opening with a discussion of the FMLA, Part II explains why the FMLA is the federal standard in the United States. Part III then describes the current Army leave policies and authorizations and aids the reader in understanding the genesis of postpartum leave in the Army. Part IV discusses corporate leave policies beyond those authorized by the FMLA, as well as state efforts to financially supplement family leave. Part IV also compares U.S. standards with international leave policies and highlights why the Army’s policies are inadequate. Part V discusses in depth the five reasons why the Army leave policy should be expanded. In Part VI, the author addresses possible counterarguments to expansion

²³ In the event of serious illness or death of an immediate family member, a Soldier may request emergency leave for up to thirty days. AR 600-8-10, *supra* note 14, para. 6-1. However, this article focuses primarily on portions of the FMLA pertaining to postpartum parental leave and will therefore only discuss leave related to childbirth.

²⁴ Expanding the entire FMLA to servicemembers, to include the provisions allowing twelve weeks to fathers for parental leave and twelve weeks to family members to care for seriously ill family members, would cause too great an impact on mission requirements than expanding portions of the FMLA.

²⁵ Current policy allows for twenty-one days leave following the adoption of a child. 10 U.S.C. § 701(i)(1) (2006). The author recommends six weeks to allow for various factors involved with adoption procedures, to include travel and minimum stay requirements in foreign adoptions, as well as bonding issues.

²⁶ *Army Family Covenant*, *supra* note 2.

of the Army leave policy. Finally, Part VII concludes with recommendations and a proposal.

II. The Family and Medical Leave Act

A. Overview

The FMLA mandates that certain employers provide eligible employees with up to twelve weeks of unpaid leave during any twelve-month period for the birth, adoption, or foster care placement of a son or daughter; to care for a spouse, parent, or son or daughter with a serious health condition; or “[b]ecause of a serious health condition that makes the employee unable to perform the functions of the position of such employee.”²⁷ Except for certain exempt employees,²⁸ employers must restore employees to their original position of employment or “an equivalent position with equivalent employment benefits, pay, and other terms and conditions of employment.”²⁹ “[T]he employer shall maintain coverage under any ‘group health plan’ . . . for the duration of such leave at the level and under the conditions coverage would have been provided if the employee had continued in employment continuously for the duration of such leave.”³⁰ If an employee does not return to work after taking leave, “[t]he employer may recover the premium that the employer paid . . . during any period of unpaid leave”³¹ Small businesses with “less than fifty employees” are exempt from providing FMLA benefits to its employees.³²

B. Background

Two months following the birth of her daughter in 1982, Lillian Garland attempted to return to her position as a receptionist with

²⁷ 29 U.S.C. § 2612(a) (2006).

²⁸ *Id.* § 2614(b). Exempt employees include, “salaried eligible employee[s] who [are] among the highest paid ten percent of the employees employed by the employer within seventy-five miles of the facility at which the employee is employed.” *Id.* The employee must also be “necessary to prevent substantial and grievous economic injury to the operations of the employer,” and “employer[s] must] notif[y] the employee of the intent of the employer to deny restoration” *Id.*

²⁹ *Id.* § 2614(a).

³⁰ *Id.* § 2614(c)(1).

³¹ *Id.* § 2614(c)(2).

³² *Id.* § 2611(2)(B)(ii).

California Federal Savings and Loan Association (Cal Fed).³³ Her employer informed her “that her job had been filled and that there were no receptionist or similar positions available.”³⁴ Ms. Garland filed a complaint claiming Cal Fed had violated § 12945(b)(2) of California’s Fair Employment and Housing Act³⁵ that required Cal Fed to reinstate her after she returned from pregnancy leave.³⁶ Cal Fed brought an action in the U.S. District Court for the Central District of California seeking both “a declaration that § 12945(b)(2) [was] inconsistent with and preempted by Title VII [of the Civil Rights Act of 1964] and an injunction against enforcement of the section.”³⁷ The district court found in favor of Cal Fed stating that providing such rights to women based on “pregnancy, childbirth, or related medical conditions [is] preempted by Title VII and [is] null, void, invalid and inoperative under the Supremacy Clause of the U.S. Constitution.”³⁸ Although the U.S. Court of Appeals for the Ninth Circuit and the U.S. Supreme Court ultimately overturned the district court’s decision,³⁹ the district court’s decision gave birth to the FMLA and encouraged the law’s initiators to develop a non-gender-based family medical leave policy.⁴⁰

In the law, Congress set forth several findings warranting the passage of the FMLA. “[T]he number of single parent households and two-parent households in which the single parent or both parents work [had] increase[ed] significantly.”⁴¹ Society had simultaneously recognized the importance of having both parents participate in early childrearing on the development of children. However, “the lack of employment policies to accommodate working parents [forced] individuals to choose between job security and parenting.”⁴² Congress likewise recognized the importance of family participation in caring for family members with

³³ *Cal. Fed. Sav. & Loan Ass’n v. Guerra*, 479 U.S. 272, 278 (1987).

³⁴ *Id.*

³⁵ CAL. GOV’T CODE § 12945(b)(2) (West 2008).

³⁶ *Cal. Fed. Sav. & Loan Ass’n*, 479 U.S. at 278.

³⁷ *Id.* at 279.

³⁸ *Id.*

³⁹ *Cal. Fed. Sav. & Loan Ass’n v. Guerra*, 758 F.2d 390, 393 (9th Cir. 1985) (“[T]he district court’s conclusion that § 12945(b)(2) discriminates against men on the basis of pregnancy defies common sense, misinterprets case law, and flouts Title VII and the PDA.”); *Cal. Fed. Sav. & Ass’n*, 479 U.S. 272.

⁴⁰ See generally RONALD D. ELVING, CONFLICT AND COMPROMISE 17–34 (1995) (providing insight to the initial family law proposal and potential sponsors).

⁴¹ 29 U.S.C. § 2601(a)(1) (2006).

⁴² *Id.* § 2601(a)(3).

serious health conditions.⁴³ Congress also found that women—more often than men—had the “primary responsibility for family caretaking,” and “such responsibility affect[ed] the working lives of women more than it affect[ed] the working lives of men.”⁴⁴ Finally, Congress specifically stated that laws protecting only women would “encourage employers to discriminate.”⁴⁵

Based on these findings, Congress intended the FMLA “to balance the demands of the workplace with the needs of families, to promote the stability and economic security of families, and to promote national interests in preserving family integrity.”⁴⁶ The FMLA is also meant to balance the needs of the employee with “the legitimate interests of employers and to minimize the potential for employment discrimination on the basis of sex by ensuring leave is available on a gender-neutral basis.”⁴⁷ The final articulated purpose of the FMLA is “to promote equal employment opportunity for women and men.”⁴⁸

Passing the FMLA proved to be an exceptionally difficult task.⁴⁹ Congress debated and revised several versions of the legislation for eight long years.⁵⁰ Supporters of the FMLA included mostly Democratic politicians representing constituents with compelling stories about balancing job security and family obligations, as well as women’s organizations, medical personnel supporting better early infant care and parental bonding, and religious organizations supporting stronger families.⁵¹ The key opponents included Republican politicians resisting Government interference with business, the National Federation of

⁴³ *Id.* § 2601(a)(2).

⁴⁴ *Id.* § 2601(a)(5).

⁴⁵ *Id.* § 2601(a)(6).

⁴⁶ *Id.* § 2601(b)(1).

⁴⁷ *Id.* § 2601(b)(3)(4).

⁴⁸ *Id.* § 2601(b).

⁴⁹ See generally ELVING, *supra* note 40 (providing a detailed analysis of the personalities, proponents, and opponents to the FMLA).

⁵⁰ See generally Parental and Disability Act of 1985 (PDLA), H.R. 2020, 99th Cong. (1985); Parental and Medical Leave Act of 1986 (PMLA), H.R. 4300, 99th Cong. (1986); Parental and Temporary Medical Leave Act of 1987, S. 249, 100th Cong. (1987); Family and Medical Leave Act of 1987 (FMLA of 1987), H.R. 925, 100th Cong. (1987); FMLA of 1989, H.R. 770, 101st Cong. (1989); FMLA of 1989, S. 345, 101st Cong.; 136 CONG. REC. H4451 (1990) (veto message of President George H.W. Bush); FMLA of 1991, H.R. 2, 102d Cong. (1991); FMLA of 1991, S. 5, 102d Cong. (1991); 138 CONG. REC. S14841, 1484–42 (1992) (veto message of President George H.W. Bush); FMLA of 1993, H.R. 1, 103d Cong. (1993); FMLA of 1993, S. 5, 103d Cong. (1993) (enacted).

⁵¹ See sources cited *supra* note 50.

Independent Business, business owners, and the National Education Association.⁵² Opponents were not against family leave, in concept, but opposed the Federal Government mandating the terms.⁵³ Additionally, during this time period, businesses were also in the process of implementing the Americans with Disabilities Act and the Civil Rights Act of 1991, which required businesses to provide handicapped-accessible facilities and to meet certain racial hiring quotas for their businesses.⁵⁴ Faced with additional mandates to provide national family leave, businesses fought the legislation and asked for the President's support. President Bush vetoed it twice.⁵⁵

What is now called the Family and Medical Leave Act was first introduced in the House of Representatives on 4 April 1985 as the Parental and Disability Leave Act of 1985.⁵⁶ Several key elements of the FMLA were debated and altered in different versions of the bill over the years, often as a result of compromise.⁵⁷ One main issue debated was the applicability of the FMLA. Those who qualified as employees varied in different bills, and employee status usually depended on the number of hours an individual had worked for an employer in the previous year.⁵⁸ The initial version did not include federal, state, or government workers.⁵⁹ The definition of employer always included any person engaged in commerce or an activity affecting commerce but varied depending on the number of employees the employer employed.⁶⁰ Some versions also featured exceptions for "highly compensated employees."⁶¹

⁵² See sources cited *supra* note 50. Many education associations were initially against mandated family leave because of concerns over "classroom disruption" and "educational mission." ELVING, *supra* note 40, at 137–38.

⁵³ *Id.*

⁵⁴ 42 U.S.C. §§ 12,101–03 (2006); 42 U.S.C. § 1981 (2006).

⁵⁵ 136 CONG. REC. H4451 (1990) (veto message of President George H.W. Bush); 138 CONG. REC. S14841, 1484–42 (1992) (veto message of President George H.W. Bush).

⁵⁶ PDLA of 1985, H.R. 2020, 99th Cong. (1985).

⁵⁷ See sources cited *supra* note 50.

⁵⁸ See *id.*

⁵⁹ H.R. 2020 §§ 101–103.

⁶⁰ See, e.g., FMLA of 1987, 100th Cong. § 101(3), (4) (1987) (defining employee as someone who had worked for employer for "not less than three consecutive months or not less than 500 hours, whichever occurs earlier"); FMLA of 1993, H.R. 1, 103d Cong. § 101(2) (1993) (defining employee as any person "employed for the last twelve months by the employer" and "for at least 1,250 hours of service in the previous twelve month period").

⁶¹ See, e.g., FMLA of 1989, H.R. 770, 101st Cong. § 106(b) (1989) (defining "highly compensated employees" as those amongst the highest paid 10% or one of the five highest paid employees).

The amount of available leave time varied from ten weeks to thirty-nine weeks and depended on the reason for and type of leave.⁶² In some versions of the bill, leave could be taken intermittently or on a reduced leave schedule.⁶³ The requirements for a qualifying serious medical condition also varied. The definition of “qualifying family members” was expanded in later versions to include parents and spouses.⁶⁴ Finally, although no version of the bill proposed paid leave, it was discussed and debated during almost every session, and proponents strongly supported its inclusion.⁶⁵

In addition to disagreements on the application of the FMLA, delays to the legislation, caused by the failure of key leadership in Congress to schedule subcommittee hearings, created further challenges.⁶⁶ In 1986, the House held hearings, but the Senate never scheduled hearings.⁶⁷ In 1987, the Senate again took no action.⁶⁸ In 1989 and 1991, after many hearings and mark-ups, Congress finally passed family leave legislation;⁶⁹ however, President H.W. Bush vetoed both versions, and the legislation did not become law. Finally, in 1993, after eight years of trying, Congress passed and the President signed this important legislation into law.⁷⁰

⁶² See, e.g., H.R. 2020, § 103(a)(2) (providing a minimum of eighteen weeks parental leave); FMLA of 1989, S. 345, 101st Cong., § 103 (1989) (providing ten weeks family leave). Other than testimony from pediatricians recommending at least twelve weeks parental bonding time, the legislative history does not provide insight to why drafters proposed the different time periods.

⁶³ See, e.g., S. 345 § 103(a)(2)(3).

⁶⁴ See, e.g., 136 CONG. REC. H2198, 2240 (1990) (amending H.R. 770 to expand family leave to cover spouses for the first time).

⁶⁵ See, e.g., *Parental and Medical Leave Act of 1986: Joint Hearing Before the Subcomm. on Civil Serv. and the Subcomm. on Compensation & Employee Benefits of the Comm. on Post Office & Civil Serv.*, 99th Cong. 131 (1986) (statement of Dr. Meryl Frank, Director, Infant Care Leave Project, Yale Bush Center in Child Development and Social Policy) [hereinafter Frank Statement].

⁶⁶ See generally ELVING, *supra* note 40 (explaining the actions taken to schedule hearings on the FMLA).

⁶⁷ See sources cited, *supra* note 50.

⁶⁸ See *id.*

⁶⁹ See *id.*

⁷⁰ 29 U.S.C. §§ 2601–2654 (2006); William J. Clinton, *Remarks on Signing the FMLA of 1993* (Feb. 5, 1993), 28 WKLY. COMP. PRES. DOC. 143.

C. Current Status of the FMLA

As of 2005, “[o]ver fifty million Americans had used the FMLA to take leave from their employment.”⁷¹ Of those, 26% took leave to care for a new child.⁷² However, sixteen years after its passage, proponents of the FMLA recognize its inadequacies. In addition to regulatory concerns over qualifying conditions and intermittent leave,⁷³ the most significant deficiency of the FMLA is the inability of some individuals to take necessary leave because it is unpaid.⁷⁴ On 4 June 2009, the House of Representatives passed the Federal Employees Paid Parental Leave Act providing financial compensation for four of the twelve weeks of leave.⁷⁵ A similar version was introduced in the Senate on 29 January 2009 and referred to the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia on 19 March 2009.⁷⁶

In 2008, Congress extended eligibility of the FMLA to allow family members of military personnel to use their FMLA benefits to assist the military member with deployment preparation and care of the military member’s dependants.⁷⁷ Congress also extended the FMLA to allow immediate family members of servicemembers wounded in the Global War on Terror to take six months of unpaid leave to care for the servicemember.⁷⁸ In essence, Congress continues to afford opportunities to civilians to care for their family servicemembers, but Congress still does not extend those benefits to servicemembers to care for their own families.

⁷¹ *Roundtable Discussion: The Family and Medical Leave Act: A Dozen Years of Experience: Hearing of the Comm. on Health, Educ., Labor, & Pensions*, 109th Cong. 8 (2005) [hereinafter *Roundtable Hearing*] (statement of Debra Ness, President, National Partnership for Women & Families).

⁷² AAUW, *The Family and Medical Leave Act: Facts and Statistics*, <http://aauw.org/advocacy/laf/lafnetwork/library/FMLAstatistics.cfm> (last visited May 27, 2009).

⁷³ LINDA LEVINE, CONG. RESEARCH SERV. REPORT, *THE FAMILY AND MEDICAL LEAVE ACT: RECENT LEGISLATIVE AND REGULATORY ACTIVITY*, RL31760, at 7–10 (2008).

⁷⁴ *Id.* at 6–7.

⁷⁵ Federal Employees Paid Parental Leave Act, H.R. 626, 111th Cong. (2009).

⁷⁶ Federal Employees Paid Parental Leave Act, S. 354, 111th Cong. (2009).

⁷⁷ 29 U.S.C.S. § 2612(a)(1)(E) (LexisNexis 2008) (*amended by* National Defense Authorization Act for Fiscal Year 2008, Pub. L. No. 110-181, 122 Stat. 3 § 585(a) (2008)).

⁷⁸ *Id.* § 2612(a)(3).

III. The Army Leave Policies⁷⁹

A. Postpartum Leave

1. Convalescent Leave for Female Soldiers Following Childbirth

To understand the current status of the Army's postpartum leave policies, it is important to understand the origin of regulations applying to pregnant women in the military. Congress established the Women's Army Auxiliary Corps (WAAC) on 14 May 1942.⁸⁰ Initially, women were not technically a part of the Army, and Army Regulations did not govern WAAC members.⁸¹ However, the WAAC drafted a set of regulations that covered, among other things, discharges from service.⁸² Under these rules, "[w]omen had been discharged as soon as possible after a doctor had certified the condition [pregnancy]."⁸³ After the WAAC became the Women's Army Corps (WAC) on 1 July 1943,⁸⁴ and then a part of the Regular Army on 12 June 1948,⁸⁵ the Army continued to discharge women for pregnancy.⁸⁶ Because the law integrating the WAC into the Regular Army did not specifically address the policy of

⁷⁹ The other Armed Services' postpartum policies are similar to the Army's. All of the services provide forty-two days of convalescent leave to recover from childbirth. The Navy has the longest postpartum operational deferment of one year, whereas the Army, Air Force, and Marine Corps only provide six months. Message, 151521Z Jul 08, PTC Washington DC, subject: ALARACT 171/2008—Notification of Pending Postpartum and Adoption Deferment Policy Change [hereinafter Postpartum Deferment Policy Change]. The Coast Guard offers a two-year sabbatical to its servicemembers called the "Care for Newborn Children Program." U.S. DEP'T OF HOMELAND SECURITY, U.S. COASTGUARD, COMDTINST M1000.6A, PERSONNEL MANUAL (with Changes 1 through 41) [hereinafter COMDSTINST M1000.6A]. For several years, the Marine Corps has been providing ten days non-chargeable leave under its Permissive Temporary Additional Duty Regulation to its male servicemembers whose wives recently gave birth.

⁸⁰ An Act to Establish the Women's Army Auxiliary Corps, Pub. L. No. 77-554, 56 Stat. 278 (1942).

⁸¹ BETTIE J. MORDEN, *THE WOMEN'S ARMY CORPS 1945-1978*, at 5 (1990).

⁸² *Id.* at 138.

⁸³ *Id.*

⁸⁴ An Act to Establish the Women's Army Corps in the Army of the United States, Pub. L. No. 78-110, 57 Stat. 371 (1943).

⁸⁵ Women's Armed Services Integration Act, Pub. L. No. 80-625, 62 Stat. 356 (1948).

⁸⁶ MORDEN, *supra* note 81, at 138 (citing U.S. DEP'T OF ARMY, REG. 615-361, ENLISTED MEN, DISCHARGE MEDICAL (4 Nov. 1944); WAAC Circular 17 (29 Dec. 42); WAAC Circular 140 (citing U.S. DEP'T OF ARMY, REG. 625-361, DISCHARGE OF ENLISTED PERSONNEL, MEDICAL (14 May 1947) (C3, 23 Feb. 1949) and SPECIAL REG. 625-5-5, DISCHARGE OF WAC OFFICERS AND WARRANT OFFICERS FOR MARRIAGE AND PREGNANCY (11 Jan. 49)).

discharging women for pregnancy, President Truman issued Executive Order 10240 in 1951 authorizing the military to discharge military women “on parenthood.”⁸⁷ The services in turn made the discharges mandatory, which continued for several years.⁸⁸

In 1967, the Army conducted the ’75 Personnel Concept Study “to develop a new personnel management concept for the post-Vietnam era,” with a “focus on reducing draft calls during peacetime.”⁸⁹ In addition to other recommendations, “[t]he study also examined the idea of retaining pregnant women and mothers on active duty as a means of reducing WAC losses.”⁹⁰ However, the study concluded, “there are too many more cogent reasons for this not being permitted . . . The members of the Women’s Army Corps must possess the same degree of mobility as male soldiers,”⁹¹ and recommended women continue to be discharged when they became pregnant.⁹²

As the Women’s Rights Movement gained momentum in the late 1960s,⁹³ female servicemembers challenged pregnancy policies in court,⁹⁴ and Congress, pressure groups, and citizens alleged the military

⁸⁷ *Id.* at 140 (citing Exec. Order No. 10240 (Apr. 27, 1951), Regulations Governing the Separation from the Service of Certain Women Serving in the Regular Army, Navy, Marine Corps, or Air Force, in U.S. DEP’T OF ARMY, BULL. (14 May 1951)).

⁸⁸ *Id.* (citing U.S. DEP’T OF ARMY, REG. 615-361, ENLISTED PERSONNEL, DISCHARGE ON MARRIAGE, PREGNANCY AND PARENTHOOD (21 Sept. 1954); SPECIAL REG. 605-225-10, RELEASE OF WOMEN OFFICERS BECAUSE OF MARRIAGE, PREGNANCY, OR PARENTHOOD) (17 June 1954)).

⁸⁹ *Id.* at 228.

⁹⁰ *Id.*

⁹¹ *Id.*

⁹² *Id.* The only person to question this policy was Senator Daniel K. Inouye of Hawaii, who asked during the October 19, 1967 Senate Armed Services Committee hearing, “Why hasn’t the service done something about this? It would appear to me that by our rules and regulations, we discourage our women members to carry on without considering the normal and natural life of raising families.” *Id.* at 213.

⁹³ Federal legislation and executive actions included The Equal Pay Act of 1963, Pub. L. No. 88-38, 77 Stat. 56 (ensuring equal pay for equal work for women employed in jobs controlled by interstate commerce laws); Title VII of the Civil Rights Act of 1964, Pub. L. No. 88-352, 78 Stat. 241 (prohibiting sex discrimination in employment unless gender was a bona fide occupational qualification); and Exec. Order No. 11,246, 3 C.F.R. 339 (Sept. 24, 1965) (prohibiting sex discrimination in the Federal Government or in employment generated by federal contracts).

⁹⁴ MORDEN, *supra* note 81, at 234 (citing Interview with Brigadier General Elizabeth Hoisington, U.S. Army Retired (Nov. 3, 1980); JEANNE M. HOLME, WOMEN IN THE MILITARY, AN UNFINISHED REVOLUTION 297 (1982)).

services discriminated against women.⁹⁵ Consequently, the Army reviewed its policies involving entry and retention of pregnant servicemembers and female servicemembers with children.⁹⁶ Despite objections from key leaders in the Army,⁹⁷ effective 9 April 1971, women could request waivers for disqualification from entry and retention because of pregnancy, terminated pregnancies, and parenthood.⁹⁸

In June 1974, the Deputy Assistant Secretary of Defense for Military Personnel Policy, over opposition from the WAC and the Deputy Chief of Staff for Personnel, “directed the services to cease invoking such policies” that authorized involuntary discharge of a woman who became pregnant, became a parent, or assumed custody of a minor.⁹⁹ Accordingly, the Army made several changes to the existing regulation, to include providing that “[t]he maximum postpartum absence would be six weeks unless the surgeon general of the Army approved an extension.”¹⁰⁰ “[T]he Secretary of Defense’s general counsel appointed the Army as the executive agent to develop uniform pregnancy and parenthood policies and to draft legislation required to repeal the offending sections of the law.”¹⁰¹ Department of Defense (DoD) directed

⁹⁵ *Id.*

⁹⁶ *Id.* at 235. The Deputy Assistant Secretary of the Army for Personnel Policy and Programs, John R. Kester, “believed that, as a matter of equity, the Army should not bar married women or unwed mothers from initial enlistment or appointment or from retention.” *Id.* at 234. He directed the Deputy Chief of Staff for Personnel to amend Army Regulations. *Id.*

⁹⁷ At that time, the Under Secretary for the Army ordered the revision of Army Regulations to allow waivers for illegitimate pregnancies and responsibility for children under eighteen years of age despite the Deputy Chief of Staff for Personnel’s request for more time to “study the impact.” *Id.* at 235 (explaining Mr. Beal’s reason was to avoid “possible adverse court rulings” while allowing the Army to decide each case individually).

⁹⁸ *Id.* at 239 (citing Memorandum from Deputy Assistant Sec’y of the Army, to Sec’y, Gen. Staff, subject: Elimination of Discriminatory Provisions of Army Regulations Pertaining to Standards of Service (25 Mar. 1971)).

⁹⁹ *Id.* at 305 (citing Memorandum from Deputy Assistant Sec’y of the Army, to Assistant Sec’y of the Military Dep’ts., subject: Involuntary Separation of Women for Pregnancy and Parenthood (7 June 1974)).

¹⁰⁰ *Id.* at 306 (citing Memorandum from Deputy Chief of Staff Personnel to Deputy Assistant Sec’y of Def., subject: Involuntary Separation of Women for Pregnancy and Parenthood (5 Nov. 1974); Message 061400Z Jun 75, Dep’t of Army, subject: Interim Change to Chapters 6 and 8, Army Regulation 635-200 and the Trainee Discharge Program (implementing the policy changes)).

¹⁰¹ *Id.* (citing Memorandum from Office of the Gen. Counsel, Dept. of Def., to Sec’y of Army, subject: Misc. 1425, proposed legislation “to amend title 10, United States Code,

the Army and the Navy to implement their new policies by 15 May 1975.¹⁰²

Other changes to the Army policy included “four weeks prenatal sick-in-quarters time, an unrestricted number of days for hospitalization during childbirth, and six to eight weeks of postpartum convalescent leave.”¹⁰³ Pregnant servicemembers were not sent overseas and were temporarily deferred from overseas duty for six weeks following childbirth.¹⁰⁴ Male servicemen were also permitted to seek a twelve-week deferment from overseas duty if their wife was in “an advanced stage of pregnancy.”¹⁰⁵ Despite time lost because of pregnancy-associated leave, subsequent DoD studies indicated, “[E]nlisted men had a higher rate of lost time than women” due to “desertion, AWOL, and alcohol and drug abuse.”¹⁰⁶ Such studies resulted in “[t]he Army (and the other services) abandon[ing] their efforts to regain the authority to discharge women involuntarily for pregnancy and accept[ing] the attendant costs in time and money.”¹⁰⁷

The current Army Regulation continues to provide female Soldiers the 1974 standard of convalescent leave following childbirth.¹⁰⁸ The unit

to repeal provisions authorizing involuntary separation of women for pregnancy and parenthood.” (29 Nov. 1974). “The Judge Advocate General prepared the draft legislation.” *Id.*

¹⁰² *Id.* at 307 (citing Memorandum from Deputy Assistant Secretary of Defense to Assistant Secretary of the Depts. of Army and Navy, subject: Involuntary Separation of Women for Pregnancy and Parenthood (11 Apr. 1975)).

¹⁰³ *Id.* at 309 (citing Disposition Form Deputy Chief of Staff for Personnel to Commander, Military Personnel Ctr., subject: Study of WAC Pregnancy Cases and Female Personnel with Dependent Children, and Information Paper, Officer of the Surgeon General (13 May 1975)).

¹⁰⁴ *Id.* (citing Disposition Form, Deputy Chief of Staff for Personnel to Commander, Military Personnel Ctr., subject: Study of WAC Pregnancy Cases and Female Personnel with Dependent Children (13 May 1975); U.S. DEP’T OF ARMY, REG. 635-5 LEAVE, PASS, ADMINISTRATIVE ABSENCES AND PUBLIC HOLIDAYS (1 June 1975)).

¹⁰⁵ *Id.*

¹⁰⁶ *Id.* at 310 (citing BINKEN & BACH, WOMEN AND THE MILITARY 60 (1977)).

¹⁰⁷ *Id.*

¹⁰⁸ AR 600-8-10, *supra* note 14, para. 5-3. The author was unable to find any evidence that postpartum convalescent leave for female servicemembers has been studied or considered again since first implemented in 1974. *See* Telephone Interview with Colonel Peter Nielsen, Obstetrician and Gynecological Consultant to the Surgeon Gen. (Feb. 18, 2009) [hereinafter Nielsen Telephone Interview]; Telephone Interview with Colonel Scott Goodrich, Senior Med. Staff Officer, Health Policy & Services Directorate, Office of the Surgeon Gen. (Jan. 15, 2009); E-mail from Major Matthew Fandre, Med. Doctor, United States Army Special Operations Command, to author (Oct. 21, 2008, 22:12 EST)

and hospital commander are the approval authorities,¹⁰⁹ and the commander is required to “limit leave to the minimum amount of time essential to meet medical needs.”¹¹⁰ The commander is also required to “consider granting soldier’s request for additional accrued, advanced, and or excess leave, as appropriate.”¹¹¹ Although the regulation states, “Soldiers are authorized forty-two days after pregnancy and childbirth,”¹¹² it also states, “A commander may require early return of a soldier if that soldier’s absence will clearly have an adverse impact on readiness or operational mission of the soldier’s unit.”¹¹³ “A cognizant military health authority must determine that such action is medically acceptable.”¹¹⁴ From a medical standpoint, the six weeks of postpartum leave is focused more on the mother and not the child.¹¹⁵ Guidance regarding medical profiles for female Soldiers is contained in Army Regulation 40-501, which references AR 600-8-10.¹¹⁶ AR 40-501, *Standards of Medical Fitness*, has only one section on postpartum. Section 7-10, Postpartum profiles, states, “convalescent leave (as prescribed by AR 600-8-10) after delivery will be for a period determined by the attending physician. This will normally be for 42 days following normal pregnancy and delivery.”¹¹⁷

2. Paternity Leave

Signed by President George W. Bush on 14 October 2008, section 532 of the 2009 National Defense Authorization Act amended 10 U.S.C. § 701 to provide, “Under regulations prescribed by the Secretary concerned, a married member of the armed forces on active duty whose

(on file with author) [hereinafter Fandre e-mail]; E-mail from Lisa Young, United States Army Ctr. for Health Promotion & Preventive Med., to author (19 Jan. 2009, 23:09 EST) (on file with author); E-mail from Colonel Karen O’Brien, TRADOC Surgeon Gen., to author (9 Feb. 2009 16:43 EST) (on file with author).

¹⁰⁹ AR 600-8-10, *supra* note 14, para. 5-3.

¹¹⁰ *Id.* tbl.5-2.

¹¹¹ *Id.*

¹¹² *Id.* para. 5-7d.

¹¹³ *Id.* para. 5-7d(2). Author has not found any evidence of a commander giving less than six weeks convalescent leave.

¹¹⁴ *Id.*

¹¹⁵ Fandre e-mail, *supra* note 108.

¹¹⁶ *Id.*

¹¹⁷ U.S. DEP’T OF ARMY, REG. 40-501, STANDARDS OF MEDICAL FITNESS para. 7-10 (14 Dec. 2007) [hereinafter AR 40-501].

wife gives birth to a child shall receive 10 days of paternity leave.”¹¹⁸ This law was a FY 2010¹¹⁹ Unified Legislative Budget¹²⁰ proposal initiated by the Navy.¹²¹ In its original form, the proposal included twenty-one days of leave, which was permissive.¹²² The final legislation reduced the leave to ten days, but made it mandatory.¹²³ The DoD has not published instructions to the regulation; however, it authorized the services to implement their own instructions. The Army released its implementing instruction on 10 March 2009.¹²⁴

B. Family and Parental Leave Options

Two other leave options are available to parents. First, active component servicemembers are authorized twenty-one days adoption leave.¹²⁵ Second, ordinary leave, as governed by AR 600-8-10, is the only option available to a parent with a seriously ill newborn following six weeks of convalescent leave.¹²⁶ Ordinary leave is discretionary—the commander can deny such requests.¹²⁷ A civilian parent in the same situation can take twelve weeks of leave.¹²⁸ This is especially relevant for mothers of premature infants. In these cases, the baby often remains in the hospital for several weeks. When the infant is ready to return home, the female servicemember has no parental leave option because her convalescent leave cannot be used to care for the child beyond the

¹¹⁸ NDAA 2009, Pub. L. No. 110-417, 122 Stat. 4356, 4449 (2008).

¹¹⁹ Because it did not involve any budgetary issues, it was able to be passed through sooner than FY 2010. Telephone Interview with Jon Clark, Staff Member, Senate Armed Services Comm. (Jan. 16, 2009) [hereinafter Clark Telephone Interview].

¹²⁰ A Unified Legislative Budget proposal is a mechanism used to change the law.

¹²¹ E-mail from Lieutenant Colonel Matthew Voithofer, G-1, Compensation and Entitlements, U.S. Army, to author (Jan. 15, 2009, 14:41 EST) (on file with author).

¹²² Clark Telephone Interview, *supra* note 119.

¹²³ *Id.* (explaining the only reason for the change was negotiation).

¹²⁴ Paternity Guidance, *supra* note 22.

¹²⁵ 10 U.S.C. § 701(i)(1) (2006). This was implemented more to enable servicemembers to meet the procedural adoption requirements such as spending a certain amount of time home with a newly adopted child. It was not implemented in an effort to allow bonding time. Clark Telephone Interview, *supra* note 119.

¹²⁶ AR 600-8-10, *supra* note 14, para. 4-3.

¹²⁷ *Id.* para. 4-3(c).

¹²⁸ 29 U.S.C. § 2612(a)(1)(A–D) (2006).

forty-two days authorized after the birth. There is no option to postpone a portion of the convalescent leave for when the baby returns home.¹²⁹

IV. Corporate, International, and State Parental Leave Policies

A. Corporate Parental Leave Policies

Corporate leave policies have steadily improved over the past twenty years as more working mothers enter or remain in the workforce. In 1989, “[f]ifty-six percent of all American women and more than one-half of all mothers with infants under one year of age work[ed] outside the home.”¹³⁰ Senator Christopher Dodd explained in legislative hearings,

There were twenty-nine million two-earner families in the United States, with 25 million children, and almost 8 million single-parent families, with an equal number of children—33 million children. One out of every other child is being reared today in a family where either both parents work or only one parent is providing for that family.¹³¹

During the same year, a survey of Fortune 500 companies found that “[o]nly half the employers surveyed offer[ed] critical infant-mother ‘bonding’ leave beyond the childbirth-related disability period.”¹³² As of 2007, 59.3% of U.S. women were working,¹³³ and 71% of women in the workforce had children under the age of eighteen.¹³⁴ Statistics from a 2008 study by the Joint Economic Committee found that 75% of Fortune

¹²⁹ AR 600-8-10, *supra* note 14, para. 5-3; Nielsen Telephone Interview, *supra* note 108 (explaining servicemembers have requested such accommodations, but the commander routinely denies due to the stated purposes of the regulation).

¹³⁰ *Family and Medical Leave Act of 1989: Hearing Before the Subcomm. on Children, Family, Drugs and Alcoholism of the S. Comm. on Labor and Human Resources*, 101st Cong. 2 (1989) [hereinafter *FMLA of 1989 S. Hearing*] (statement of Sen. Dodd, Chairman, Subcomm. on Children, Family, Drugs and Alcoholism, Comm. on Labor & Human Resources).

¹³¹ *Id.*

¹³² *Id.*

¹³³ U.S. BUREAU OF LABOR SERVICES, HOUSEHOLD DATA ANNUAL AVERAGES tbl.2 (2008) [hereinafter *HOUSEHOLD DATA ANNUAL AVERAGES*] (providing employment status of the civilian non-institutional population sixteen years and over by sex from 1973 to date).

¹³⁴ U.S. BUREAU OF LABOR STATISTICS, BULL. 2307, tbl.578 (2008) (Employment Status of Women by Marital Status and Presence and Age of Children: 1997 to 2007).

100 companies offer new mothers paid maternity leave, typically lasting six to eight weeks.¹³⁵ Another study by Working Mother Media, Inc., publisher of *Working Mother Magazine*, selected the one hundred family-friendliest companies in the United States.¹³⁶ More than 28% provided nine or more weeks of paid maternity leave, and more than half provided some amount of paid paternity leave varying from one to six weeks.¹³⁷ Eighty top law firms provide at least twelve weeks of some type of compensated maternity leave.¹³⁸ The paid portion is usually broken down into two parts: short-term, insurance-paid medical leave (usually six to eight weeks), and firm-paid parental or childcare leave.¹³⁹ Additionally, the FMLA still entitles parents to take what is remaining of twelve weeks as unpaid leave.¹⁴⁰

Even though many companies offer generous benefits, many advocates argue that the FMLA should be expanded for those who are not able to work for such companies. Advocates argue that when compared to the rest of the industrialized world,¹⁴¹ the United States is out of synch. Ms. Debra Ness, President of the National Partnership for Women and Families in Washington, D.C., provided the following statement during a Senate hearing on 23 June 2005:

We live at a time when three-quarters of families
have both parents working. And we still are very badly

¹³⁵ JOINT ECONOMIC COMMITTEE, MAJORITY STAFF, PAID FAMILY LEAVE AT FORTUNE 100 COMPANIES: A BASIC STANDARD BUT STILL NOT THE GOLD STANDARD 6 (2008), *available at* <http://www.jec.senate.gov/index.cfm?FuseAction=Reports.Reports> (follow “March 2008” hyperlink; then follow “Paid Maternity Leave” hyperlink) [hereinafter JEC PAID FAMILY LEAVE].

¹³⁶ INSTITUTE FOR WOMEN’S POLICY RESEARCH, MATERNITY LEAVE IN THE UNITED STATES (2007), *available at* www.iwpr.org/pdf/parentalleaveA131.pdf [hereinafter IWPR REPORT].

¹³⁷ *Id.* at 8 (explaining some of the companies offering the best benefits include Goldman, Sachs & Co. (offering sixteen weeks of paid maternity leave, plus four weeks for new fathers and eight weeks for adoptive parents), Pillsbury Winthrop Shaw Pittman LLP (offering eighteen weeks of paid leave), Johnson & Johnson (offering twenty-six weeks of paid maternity leave to new mothers with five year tenure)).

¹³⁸ The Associate Pirate, *Maternity Leave, Part Deux*, <http://associatepirate.com/2008/02/21/maternity-leave-part-deux> (last visited Jan. 19, 2009) [hereinafter Associate Pirate].

¹³⁹ JEC PAID FAMILY LEAVE, *supra* note 135, at 8.

¹⁴⁰ Family and Medical Leave Act of 1993, 29 U.S.C. § 2612(a) (2006).

¹⁴¹ Jamie L. Hartman, *House Passes Paid Parental Leave Bill; President Expected to Veto*, OHMYGOV!, June 20, 2008, http://ohmygov.com/blogs/general_news/archive/2008/06/20/house-passes-paid-parental-leave-bill-president-expected-to-veto.aspx (explaining more than 163 industrialized nations guarantee paid maternity leave, and forty-five of those also provide paid paternity leave).

out of sync with the realities that most working families face because we still primarily operate as a society on the assumption that there is still a full-time caregiver at home. We as a Nation care a great deal about family values and I think the FMLA was a step toward putting those values into action in ways that really support families.

Since its enactment, 50 million Americans have taken advantage of the FMLA; 42 percent of those have been men, 58 percent of those have been women. And we know from some of the research that has been done that many of those individuals say that it led to quicker recoveries, it led to their ability to follow doctor's orders more carefully, it led to avoidance of parents being put into nursing homes. And we also know that 98 percent of employees who have taken advantage of FMLA have returned to the same employer.¹⁴²

Similarly, another professional expert who advocated for the implementation of the FMLA during the eight years it was debated in Congress was Dr. Meryl Frank, then the Director of the Infant Care Leave Project, Yale Bush Center in Child Development and Social Policy. Dr. Frank testified regarding the findings of the Yale Bush Center Advisory Committee on Infant Care Leave, which recommended passage of

policies which would allow employees a leave of absence for a period of time sufficient to enable mothers to recover from pregnancy and childbirth and parents to care for newborn or newly adopted infants. Such a leave would provide income replacements, benefit continuation and job protection. The leave would be available to either mother or father for a minimum of six months, and would include partial income replacement (75% of salary) for three months, up to a realistic maximum benefit sufficient to assure adequate basic resources for the families who need them most. Benefit

¹⁴² Roundtable Hearing, *supra* note 71, at 8.

continuation and job protection would be available for the entire six-month leave period.¹⁴³

The military should take these statistics and policy recommendations into consideration in establishing more family-friendly parental leave policies. The demographics of families in the military are similar to those of civilians. More male servicemembers have working spouses, requiring male servicemembers to be more involved in parenting than in previous generations. More importantly, 38.1% of all females in the Army are married to other servicemembers.¹⁴⁴ If the military does not keep pace with the benefits civilian companies offer to retain their own most talented employees, the military will continue to lose talented servicemembers.

B. International Parental Leave Policies

The FMLA provides for less parental leave than any other industrialized nation.¹⁴⁵ The U.S. military provides even less than the FMLA.¹⁴⁶ In the 1970s, after the U.S. Army started allowing female servicemembers to remain in the military following childbirth, nine European countries were already increasing job-protected paid leave on average from ten to twenty-six weeks and full-pay weeks from eight to twenty-one weeks.¹⁴⁷ The European Union mandates a minimum of fourteen weeks paid parental leave.¹⁴⁸ In Canada, mothers receive “job protection and benefit entitlement” for a maximum of one year in most provinces.¹⁴⁹ “Income replacement for maternity leave in Canada is

¹⁴³ Frank Statement, *supra* note 65.

¹⁴⁴ U.S. DEP'T OF THE ARMY, DEPUTY CHIEF OF STAFF OF PERSONNEL, OFFICE OF ARMY DEMOGRAPHICS, FY08 ARMY PROFILE (2008) [hereinafter FY08 ARMY PROFILE] (on file with author).

¹⁴⁵ *Family and Medical Leave Act of 1989: Hearing Before the Comm. of the Whole House on the State of the Union*, 101st Cong. 27 (1990) (statement of Rep. George Miller, Democratic Congressman, explaining twenty-four African countries, nine Asian countries, seven Middle Eastern countries, nineteen European countries and fourteen Central American countries have maternity leave, and most offer paid leave).

¹⁴⁶ AR 600-8-10, *supra* note 14, para. 5-3 (providing forty-two days convalescent leave); 29 U.S.C. §§ 2612(a) (2006) (providing twelve weeks parental leave).

¹⁴⁷ Christopher J. Ruhm, *Parental Leave and Child Health*, 19 J. OF HEALTH ECON. 931, 942-43 (2000).

¹⁴⁸ Katharina Staehelin et al., *Length of Maternity Leave and Health of Mother and Child—A Review*, 52 INT. J. PUB. HEALTH 202, 202 (2007).

¹⁴⁹ Michael Baker et al., *Maternal Employment, Breastfeeding, and Health: Evidence from Maternity Leave Mandates*, 27 J. OF HEALTH ECON. 871, 872 (2008).

governed by the Employment Insurance program. Most other terms of the leave, including job protection, are determined by provincial labor market standards.”¹⁵⁰ In Sweden, parents are authorized approximately eighteen months of parental leave, and leave can be shared between the mother and the father.¹⁵¹ Germany provides fourteen weeks of paid maternity leave, and France provides sixteen weeks, both with one hundred percent wage replacement.¹⁵² “In Great Britain, 90% of wages are provided for the first six weeks, with a flat rate thereafter for a minimum total of fourteen weeks. Mothers in Norway may receive either 100% paid maternity leave for forty-two weeks, or 80% paid leave for fifty-two weeks.”¹⁵³

The military in these countries extend these same benefits to their servicemembers.¹⁵⁴ A 2009 comparative report on reproductive health studying eight navies found the U.S. Navy offered the least maternity leave to its servicemembers.¹⁵⁵ The country offering the second lowest amount of maternity leave was Germany, which provides fourteen weeks paid maternity leave—eight weeks more than the United States. The U.S. military is shamefully behind both civilian corporations and other countries in providing necessary parental leave to new parents.

¹⁵⁰ *Id.* at 874.

¹⁵¹ See Asa Premberg et al., *Experiences of the First Year as Father*, 22 SCAND. J. CARING SCI. 56, 56 (2008).

¹⁵² Ruhm, *supra* note 147, at 938.

¹⁵³ Gerald Calnen, *Paid Maternity Leave and Its Impact on Breastfeeding in the United States: An Historic, Economic, Political, and Social Perspective*, 2 BREASTFEEDING MED. NO. 1, at 34, 39 (2007).

¹⁵⁴ See, e.g., GREAT BRITAIN DEFENSE INSTRUCTIONS AND NOTICES, MATERNITY ARRANGEMENTS FOR SERVICEWOMEN IN THE REGULAR ARMED FORCES para. 18 (Jan 2007) (on file with author) (providing fifty-two weeks total maternity leave, of which twenty-six weeks are paid); Lakshmi Fjord et al., *Reproductive Health in Eight Navies: A Comparative Report on Education, Prevention Services, and Policies on Pregnancy, Maternity/Paternity Leaves, and Childcare*, 174 MIL. MED. NO. 3, at 278 (2009); Telephone Interview with Major Marla Dow, Canadian Army, The Judge Advocate Gen.’s Legal Ctr. & Sch. (Mar. 12, 2009) (explaining the Canadian military follows the civil code and provides a year paid maternity leave, most often back-filled by a reservist); Telephone Interview with Mr. Thomas Nix, German Liaison to The Judge Advocate Gen.’s Legal Ctr. & Sch. (Mar. 12, 2009) (explaining the German military follows the civil code and provides fourteen weeks paid maternity leave).

¹⁵⁵ Fjord et al., *supra* note 154, at 285.

C. State Parental Leave Policies

As a result of inadequate compensation, which prevents many parents from using FMLA leave, six states and Puerto Rico have introduced paid family leave programs.¹⁵⁶ California uses a combination of leave sources to provide parental leave, to include State Disability Insurance, Parental Leave, and most recently, the Family Temporary Disability Insurance (FTDI).¹⁵⁷ In addition to ten weeks of pregnancy-related leave, employees that contribute to FTDI receive up to 5% of their wages for six weeks.¹⁵⁸ New Jersey also provides six weeks of partial wage-replacement in addition to pregnancy-related leave.¹⁵⁹ Similarly, Hawaii, New York, and Rhode Island have Temporary Disability Insurance programs that provide six weeks of wage replacement.¹⁶⁰ Washington provides five weeks of partially paid leave,¹⁶¹ and Illinois recently introduced a Family Leave Insurance Program that would allow for four weeks paid family leave.¹⁶²

The time is ripe for military leaders and Congress to fully review postpartum leave policies for its servicemembers. The next section of this article details several reasons supporting longer parental leave.

V. Reasons Supporting Longer Postpartum Leave

Providing longer parental leave to servicemembers will benefit all facets of the "Army Team." The infant children of servicemembers will benefit by improved health. The health of parent servicemembers will likewise improve. This improved health of parent and child will lead to improved psychological health and bonding between both parent and child and improved infant development. In turn, this will lead to better performance at work by the postpartum parents. Finally, expanding postpartum leave policies will benefit the Army as a whole as it will lead to better performance, more loyal service, and improved retention rates.

¹⁵⁶ Calnen, *supra* note 153, at 38; JEC PAID FAMILY LEAVE, *supra* note 134, at 12.

¹⁵⁷ Nina Fendel et al., *California's New Paid Family Leave Law: Family Temporary Disability Insurance (FTDI)*, 10 CPER J. 161 (2003).

¹⁵⁸ *Id.* at 11.

¹⁵⁹ 2008 N.J. Laws 17.

¹⁶⁰ JEC PAID FAMILY LEAVE, *supra* note 135, at 13.

¹⁶¹ *Id.*

¹⁶² *Id.*

A. Infant Health

1. Generally

Parental leave policies providing at least two to three months of paid leave improve the health of children.¹⁶³ One study determined “an extra week of paid maternity leave correlates with a 2% to 3% reduction in infant mortality rates,”¹⁶⁴ but even as recently as 2000, there were very few studies on the relationship between parental leave entitlements and infant health.¹⁶⁵ In 2000, Christopher Ruhm published results from a study using data from sixteen European countries collected between 1969 and 1994.¹⁶⁶ He found that rights to parental leave are associated with substantial decreases in pediatric mortality:

In particular, there is a much stronger negative relationship between leave durations and either post-neonatal mortality (deaths between 28 days and 1 year of age) or child fatalities (deaths between the first and fifth birthday) than for perinatal mortality (fetal deaths and deaths in the first week), neonatal mortality (deaths in the first 27 days), or in the incidence of low birth weight.¹⁶⁷

Ruhm further found, “A ten-week increase in paid leave is predicted to reduce infant mortality rates by between 2.5% and 3.4%. By contrast, unpaid leave is unrelated to infant mortality, which makes sense if parents are reluctant to take time off work when wages are not replaced.”¹⁶⁸ Additionally, “a year of job-protected paid leave [is] associated with roughly a twenty percent decline in post-neonatal deaths and a fifteen percent decrease in fatalities occurring between the first and fifth birthdays.”¹⁶⁹ Ruhm’s study examined the leading causes of post-neonatal and child deaths in the United States and concluded, “[F]our of

¹⁶³ Ruhm, *supra* note 147, at 931.

¹⁶⁴ *Id.* at 932 (citing C.R. Winegarden et al., *Demographic Consequences of Maternal-Leave Programs in Industrialized Countries: Evidence from Fixed-Effect Models*, 61 S. ECON. J. 1020–35 (1995)).

¹⁶⁵ *Id.*

¹⁶⁶ *See id.*

¹⁶⁷ *Id.* at 933. Ruhm also found these same “leave entitlements are also unrelated to the death rates of senior citizens, suggesting that the models adequately control for unobserved influences on health that are common across ages.” *Id.*

¹⁶⁸ *Id.* at 947.

¹⁶⁹ *Id.* at 952.

the five leading causes of post-neonatal mortality (Sudden Infant Death Syndrome, accidents, pneumonia/influenza, and homicide) account[ed] for forty-three percent of the fatalities, [and] are almost certainly substantially influenced by activities of parents.”¹⁷⁰ Ruhm concluded:

Closer parental involvement is likely to prevent some accidental deaths and may indirectly reduce other sources of fatalities. For example, SIDS is more than twice as common among infants who sleep prone as for those who do not Parental leave could increase the frequency of non-prone sleeping if parents have more energy to monitor sleeping position or are more able to directly observe it. Time off work might also decrease homicides by reducing stress levels in families with young children. Finally, parental leave might lessen the need for child care, which is associated with increased risk of many infectious illnesses Parental inputs may even influence mortality due to congenital anomalies to the extent they determine whether the child receives timely medical treatment and other health-preserving investments.¹⁷¹

Like the infant in our opening scenario, studies have found that young children who attend daycare are at increased risk for infections.¹⁷² One particular study determined that at age two, “frequent wheezing was significantly higher among children with greater exposure to other children at home or at day care than among those with less exposure to other children (24% v. 17%).”¹⁷³ This was particularly true of children who entered daycare before the age of six months.¹⁷⁴ “[A]mong four-to-five year old children, daycare attendance also increased the risk of

¹⁷⁰ *Id.* at 954.

¹⁷¹ *Id.*

¹⁷² See Thomas M. Ball et al., *Siblings, Daycare Attendance, and the Risk of Asthma and Wheezing During Childhood*, 343 NEW ENG. J. MED. NO. 8, at 538, 538 (2000); see also Michael T. Osterholm, *Infectious Disease in Child Day Care: An Overview*, 94 PEDIATRICS NO. 6, at 987 (1994); Catherine J. Holberg et al., *Child Daycare, Smoking by Caregivers, and Lower Respiratory Tract Illness in the First 3 Years of Life*, 91 PEDIATRICS NO. 5, at 885 (1993) (finding the presence of three or more unrelated children in the care setting was a significant independent risk factor for lower respiratory illness during the first three years of life).

¹⁷³ Ball et al., *supra* note 172, at 541.

¹⁷⁴ *Id.*

asthma.”¹⁷⁵ While this study also acknowledges that exposure to other children as a newborn provides important signals to the newborn’s maturing immune system,¹⁷⁶ the study does not address the effect being exposed to bacterial and viral infections has on the youngest of infants; it only acknowledges that infants experience more adverse health effects.¹⁷⁷

Exposure to infection is not the only risk. “Lower respiratory tract illness (LRI) is one of the main causes of morbidity in infancy and early childhood in the United States, accounting for a substantial proportion of office visits to pediatricians and hospitalizations.”¹⁷⁸ One study determined, “The cumulative LRI incidence rates (first, second, and third LRIs) in the first 3 years of life for those infants with the longest daycare experience are significantly higher than those for other child care experience groups.”¹⁷⁹ Another study found, “In children less than one year of age, the first six months of enrollment in the first childcare facility were associated with a 69% higher incidence of hospitalizations for acute respiratory infection compared with children in home care.”¹⁸⁰ This study recommended postponing enrollment into childcare until after the age of one.

2. Breastfeeding

In addition to the direct benefit of improved health of a baby who is home with a parent, infants are also healthier if they are breastfed for at least the first year of life.¹⁸¹ Longer maternity leave is directly linked to mothers’ breastfeeding of infants for longer periods.¹⁸² The benefits of

¹⁷⁵ *Id.* at 542.

¹⁷⁶ *Id.* But see Holberg et al., *supra* note 172 (concluding prolonged daycare did not protect against lower respiratory illnesses in the third year of life).

¹⁷⁷ Ball et al., *supra* note 172, at 541.

¹⁷⁸ Holberg et al., *supra* note 172, at 885; see also Laurens P. Koopman et al., *Respiratory Infections in Infants: Interaction of Parental Allergy, Child Care, and Siblings—The PIAMA Study*, 108 PEDIATRICS NO. 4, at 943 (2001) (determining child care attendance or having siblings increased the risk of developing doctor-diagnosed LRTI in the first year of life).

¹⁷⁹ Holberg et al., *supra* note 172, at 891. Other child care groups include those without prolonged childcare experience.

¹⁸⁰ See generally Mads Kamper-Jorgensen et al., *Population-Based Study of the Impact of Childcare Attendance on Hospitalizations for Acute Respiratory Infections*, 110 PEDIATRICS NO. 4, at 1439 (2006).

¹⁸¹ See generally American Academy of Pediatrics, *Policy Statement on Breastfeeding and the Use of Human Milk*, 115 PEDIATRICS NO. 2, at 496 (2005).

¹⁸² Baker et al., *supra* note 149, at 872.

breastfeeding on infant health are so great that public health agencies have renewed efforts to promote breastfeeding.¹⁸³

In 1997, the American Academy of Pediatrics summarized the benefits of breastfeeding, citing 111 research articles, in support of a new set of breastfeeding guidelines (American Academy of Pediatrics, 1997). The reported benefits for children include decreases in diarrhea, otitis media (ear infections), gastro-intestinal diseases, asthma, lower respiratory infections, sudden infant death syndrome, lymphoma, and chronic digestive diseases. For mothers, the benefits include an earlier return to pre-pregnancy weight, improved bone remineralization, and a reduced risk of ovarian and premenopausal breast cancer.¹⁸⁴

Unfortunately, the rates of women still breastfeeding at three, six, and twelve months are still very low.¹⁸⁵ Nationwide, as of 2008, 74.2% of women initiated breastfeeding, 43.1% were still breastfeeding at six months, but only 11.9% were exclusively breastfeeding at six months.¹⁸⁶ These numbers continue to fall short of the Healthy People 2010 objectives.¹⁸⁷ “Mothers report the need to return to work is the leading reason to stop breastfeeding at longer durations.”¹⁸⁸

One of the primary reasons women do not initiate breastfeeding immediately following childbirth is because of the need to return to work.¹⁸⁹ “There is a significant relationship between breastfeeding initiation rates and return to work within 6 weeks of delivery; those mothers returning so soon after giving birth were significantly less likely

¹⁸³ *Id.* at 871; *see also* Healthy People 2010 Initiative, <http://www.healthfinder.gov/scripts/SearchContext.asp?topic=129> (last visited Jan. 19, 2009) (explaining the “Healthy People Goal” is to reach a level of seventy-five percent breastfeeding in the early postpartum period, fifty percent at six months, and twenty-five percent at one year).

¹⁸⁴ Baker et al., *supra* note 149, at 873.

¹⁸⁵ DEP’T OF HEALTH & HUMAN SERVS. CTRS. FOR DISEASE CONTROL & PREVENTION, BREASTFEEDING REPORT CARD—UNITED STATES, 2008, at 2–4 (2008), *available at* http://www.cdc.gov/breastfeeding/data/report_card.htm [hereinafter CDC].

¹⁸⁶ *Id.* at 2.

¹⁸⁷ *Id.* at 1. Healthy People 2010 is a description of the nation’s health priorities.

¹⁸⁸ Baker et al., *supra* note 149, at 872; Telephone Interview with Katie Chisolm, Lactation Consultant at Fort Bragg, N.C. (Mar. 10, 2009).

¹⁸⁹ Baker et al., *supra* note 149, at 873 (citing B. HAMLYN ET AL., INFANT FEEDING 2000 (2002)).

to choose to breastfeed.”¹⁹⁰ The longer a woman is able to remain home with her infant before returning to the workforce directly correlates to the length of time the woman continues breastfeeding.¹⁹¹ The Baker study examined breastfeeding rates following an increase in maternity and parental leave entitlements in Canada from six months to one year of job-protected, compensated maternity leave.¹⁹² The study found that when the amount of maternity leave women could take increased, breastfeeding duration also increased substantially.¹⁹³ Therefore, the proportion of mothers entitled to longer maternity leave, who attained the public health benchmark¹⁹⁴ of six months of exclusive breastfeeding, increased by nearly 40%.¹⁹⁵

“At least 50% of women who are employed when they become pregnant return to the labor force by the time their children are 3 months old.”¹⁹⁶ In the military, almost 100% of women return to the workforce by the time their children are between the ages of six and eight weeks.¹⁹⁷ “National norms, however, indicate that only 10% of employed mothers continue feeding their infants breastmilk for the recommended first 6 months of life.”¹⁹⁸ It is likely that military statistics are similar to national norms of other working women, with only 10% of active

¹⁹⁰ Calnen, *supra* note 153, at 34 (citing S. Noble, *Maternal Employment and the Initiation of Breastfeeding*, 90 ACTA PAEDIATRICA 423 (2001)).

¹⁹¹ See C.R. Arthur et al., *The Employment-Related Breastfeeding Decisions of Physician Mothers*, 44 J. MISS. STATE MED. ASS'N No. 12, at 383 (1999); B. Roe et al., *Is There Competition between Breastfeeding and Maternal Employment*, 36 DEMOGRAPHY No. 2, at 157 (2002); G. Yilmaz et al., *Factors Influencing Breastfeeding for Working Mothers*, 44 TURK J. PEDIATRICS No. 1, at 30 (2002).

¹⁹² Baker et al., *supra* note 149, at 872.

¹⁹³ *Id.*

¹⁹⁴ *Id.* at 871 (explaining the World Health Organization recommends six months of exclusive breastfeeding; the U.S. Department of Health and Human Services recommends six months of exclusive breastfeeding, with continued feeding to one year; and Health Canada recommends six months exclusive feeding, with continued feeding up to age two and beyond).

¹⁹⁵ *Id.* at 884.

¹⁹⁶ Rona Cohen et al., *Comparison of Maternal Absenteeism and Infant Illness Rates Among Breast-Feeding and Formula-Feeding Women in Two Corporations*, 10 AM. J. OF HEALTH PROMOTION No. 2, at 148, 149 (1995).

¹⁹⁷ AR 40-501, *supra* note 117, para. 7-10; AR 600-8-10, *supra* note 14, para. 5-3. This percentage omits the number of female servicemembers who choose to voluntarily separate either by ETS prior to childbirth or by U.S. DEP'T OF ARMY, REG. 635-20, ACTIVE DUTY ENLISTED ADMINISTRATIVE SEPARATIONS para. 5-8 (6 June 2005).

¹⁹⁸ Cohen et al., *supra* note 196, at 149.

component servicemembers still breastfeeding their infants six months after childbirth.¹⁹⁹

One study determined that one demographic is most likely to combine full-time employment and breastfeeding: “women older than 25 years of age, well-educated (college), in a higher income group (>\$25,000), and living in the western portion of the United States.”²⁰⁰ This is not the demographic of a majority of the Army’s enlisted corps. Combined with the additional challenge of having to return to work six weeks sooner than civilian counterparts entitled to FMLA leave, enlisted servicemembers are much less likely to breastfeed their children for the recommended periods of time.²⁰¹

This is significant because studies indicate infants and young children are less likely to get infections and illnesses if they are breastfed longer.²⁰² One study, comparing infants fed formula to infants fed almost exclusively breast milk, showed that 86% of the total infants that did not have any illnesses were from the breastfed sample.²⁰³ Furthermore, of all the illnesses in this study requiring a one-day absence from work, “[t]wenty-five percent occurred in breast-fed babies and 75%

¹⁹⁹ The author was unable to find any statistics on percentages of female servicemembers breastfeeding. The author contacted numerous military treatment facilities (MTFs) and obstetric and pediatric specialists to include the Senior Medical Staff Officer for Health Policy & Services at the Office of the Surgeon Gen.; the policy advisor to the OSG; Chief of Midwifery, Fort Bragg, N.C.; Lactation Specialists at Fort Bragg, N.C. and Fort Drum, N.Y.; Chief of Obstetrics & Gynecology at Fort Lewis, Wash.; the Ass’n of Military Surgeons of the U.S. (AMSUS) Representative to the United States Breastfeeding Comm. (USBC); and, the U.S. Army Ctr. for Health Policy & Preventive Health and found this data is not tracked. Generally and anecdotally, MTFs seem to reflect the community where they are located. E-mail from Captain Julia D. Block, U.S. Navy, AMSUS Representative, USBC to author (Mar. 5 2009, 0010 EST) (on file with author).

²⁰⁰ Cohen et al., *supra* note 196, at 149 (citing A.S. Ryan et al., *Breastfeeding and the Working Mother: A Profile*, 83 PEDIATRICS 524 (1989)).

²⁰¹ The Air Force is the only branch with a regulation addressing breastfeeding in the work environment. In 2005, the Air Force recommended supervisors of breastfeeding Air Force members allow fifteen to thirty minutes every three to four hours to pump breast milk in an area with adequate privacy and cleanliness. Restrooms are specifically mentioned as an inappropriate location to pump. The reason stated is that the “importance of breastfeeding during the first year of life to infant nutrition and health and to family emotional support is recognized by numerous private and governmental authorities.” U.S. DEP’T OF AIR FORCE, INSTR. 44-102, MEDICAL CARE MANAGEMENT para. 4.15 (1 May 2006).

²⁰² The author was unable to find any evidence of any organization recommending formula over breast milk.

²⁰³ See generally Cohen et al., *supra* note 196.

in formula-fed babies.”²⁰⁴ Another study determined, “An extra week of postpartum job absence raises the duration of breast-feeding by 3 to 4 days, with an accompanying growth in frequency for those who do so [initiate breast-feeding].”²⁰⁵ The same study examined available evidence on the effects of such increased breastfeeding rates on the reduction of infant deaths. Evidence showed that “[a] 30 percentage point increase in the fraction of women intending to breast-feed was estimated to decrease post-perinatal death rates by more than 9%.”²⁰⁶ The study also determined that “[b]reast-feeding is associated with a 3.7 per thousand fall in post-perinatal mortality”²⁰⁷

The Army does not have a formal policy on breastfeeding, but the U.S. Army Surgeon General and Medical Services Corps encourage female dependants and servicemembers to breastfeed. However, the Soldier must solicit support and gain permission from her commander to breastfeed at work.²⁰⁸ Some posts have a program designed specifically for working mothers that enables mothers to borrow a breast pump, at no cost, to help facilitate expressing their milk while at work.²⁰⁹ While such programs are encouraging, they do not appear to change the statistics showing that the number one reason for choosing not to breastfeed, or to stop breastfeeding prior to the recommended six months, is due to early return to the work force. A more scientifically proven way to encourage more women to breastfeed is to extend maternity leave.

²⁰⁴ *Id.* at 152.

²⁰⁵ Ruhm, *supra* note 147, at 952 (citing Roe et al., *supra* note 191).

²⁰⁶ *Id.* (citing R.G. Carpenter et al., *Prevention of Unexpected Infant Death; An Evaluation of the First Seven Years of the Sheffield Intervention Program*, 83297 LANCELOT 723 (1983)).

²⁰⁷ *Id.* (citing A.S. Cunningham, *Breastfeeding and Health in the 1980s; A Global Epidemiologic Review*, 118 J. PEDIATRICS 659 (1991)).

²⁰⁸ See, e.g., Memorandum from Breastfeeding Servicemember to Commander, subject: Breastfeeding Support Plan on Return to Duty; Memorandum from Breastfeeding Servicemember, to Commander, subject: Breastfeeding Work Plan, *available at* <http://chppm-www.apgea.army.mil/dhpw/Population/SamplebreastfeedingmemocommanderFINAL0807.pdf>. (Sample memorandums available on the U.S. Army Ctr. for Health Promotion & Preventive Med. for servicemembers to present to their commanders), *available at* <http://chppm-www.apgea.army.mil/dhpw/Population/SamplebreastfeedingmemocommanderFINAL0807.pdf>.

²⁰⁹ E-mail from Lieutenant Colonel Noelle Briand, S3, 4th Psychological Operations Group, U.S. Army, to author (9 Mar. 2009) (on file with author) (describing program at Fort Bragg, N.C.).

B. Parent Health

Besides improved infant health associated with periods of longer maternity leave, improved parent health has also been linked to longer maternity leave. “Many first-time mothers find that the real experience of recovering from childbirth, while assuming the role of mother and resuming previous roles is more like a bad dream than the anticipated fairy tale.”²¹⁰ New parents seldom get enough sleep during the first few months of their child’s life. One study found, “Postpartum fatigue is progressive in nature and continues beyond the traditional 6-week postpartum period.”²¹¹

In addition to increased opportunity for rest, extending postpartum leave can positively affect a new mother’s mental and emotional health. One review examined thirteen original studies on the length of maternity leave, the mother’s mental health, and the duration of breastfeeding.²¹² The review classified short leaves as those lasting eight to twelve weeks.²¹³ It compared short leaves with a reference group of mothers taking only six to nine weeks of maternity leave.²¹⁴ The review found that a mother who takes leave for eight to twelve weeks has “[a] decrease in maternal depressive symptoms, an improvement in the quality of mother-infant interactions, better vitality, as well as longer breastfeeding durations . . .” compared with a mother taking only six to nine weeks of maternity leave.²¹⁵ Another study determined that short to moderate periods away from work (considered twelve to twenty weeks in this

²¹⁰ Nancy Wieland Troy, *A Comparison of Fatigue and Energy Levels at 6 Weeks and 14 to 19 Months Postpartum*, 8 CLINICAL NURSING RES. No. 2, at 135, 135 (1999) (citing D.K. Gjerdingen et al., *Changes on Women’s Physical Health During the First Postpartum Year*, 2 ARCHIVES OF FAM. MED. 277–83 (1993); R.A. Milligan, *Maternal Fatigue During the First Three Months of the Post-partum Period* (1989) (unpublished doctoral dissertation, University of Maryland, Baltimore); N.W. Troy et al., *The Development of a Self-care Guide for Postpartum Fatigue*, 8 APPLIED NURSING RES. 92–96 (1995)).

²¹¹ Troy, *supra* note 210, at 136. Of note, only 21% of the women studied were working at six weeks postpartum and only an average of forty hours per week. With a military duty day beginning for most at 0630 and ending at 1715, mothers returning to work in the military start working a fifty-four hour work week just six weeks after giving birth.

²¹² See Staehelin et al., *supra* note 148.

²¹³ *Id.* at 207. What is classified as a short leave is actually two to four weeks longer than what is available to active component servicemembers.

²¹⁴ *Id.* at 208.

²¹⁵ *Id.* at 207–08.

study), are associated with worse mental health, vitality and role function than longer periods of more than twenty weeks.²¹⁶

Doctors recommend a minimum of six to eight weeks off after childbirth to recover physically.²¹⁷ This time is considered maternity disability. It does not account for the time necessary to adjust mentally and emotionally to parenthood while simultaneously battling fatigue and employment requirements. Increasing maternity leave would have a long-term positive effect on the mental health of servicemembers who have recently given birth by allowing them adequate time to adjust to balancing parenthood and military service.

C. Psychology, Development, and Bonding

“Much has been learned about the profound psychological, emotional, and physiologic dependence of the infant upon the mother during the first months of life, and its crucial impact on long-term physical and mental health.”²¹⁸ Shorter maternity leaves have a detrimental effect on the relationship between the infant and the mother. One study showed,

Four months after childbirth, mothers entitled to short maternity leaves (6 weeks) showed significantly more negative interactions with their infant than women with longer maternity leaves (12 weeks). In addition, women with more physical health symptoms, elevated levels of depressive symptoms, or having a child with a difficult temperament, interacted significantly less positively with their child if they were entitled to only 6 weeks of maternity leave than comparable women entitled to 12 weeks of leave.²¹⁹

²¹⁶ *Id.* at 205 (citing P. McGovern et al., *Time Off Work and the Postpartum Health of Employed Women*, 35 MED. CARE NO. 5, at 507 (1997)).

²¹⁷ *PDLA H.R. Hearing*, *supra* note 7 (statement of Ms. Sheila B. Kamerman, Professor, Columbia University School of Social Work).

²¹⁸ Staehelin et al., *supra* note 148, at 208 (citing A.N. Schor, *Back to Basics: Attachment, Affect Regulation, and the Developing Right Brain: Linking Developmental Neuroscience to Pediatrics*, 26 PEDIATRIC REV. 204 (2005)).

²¹⁹ *Id.* at 205 (citing R. Clark et al., *Length of Maternity Leave and Quality of Mother-Infant Interactions*, 68(2) CHILD DEV. 364 (1997)).

In 1985, during one of the first committee hearings for the FMLA, Dr. Berry Brazelton spoke about strengthening families.²²⁰ Dr. Brazelton is one of the most noted child development experts in the world.²²¹ He testified extensively throughout the eight years of FMLA hearings on two main aspects of separating infants and mothers prematurely: (1) the development of working families and (2) infant development.²²² He reiterated that labor statistics showed women as a key force in the labor market and argued that the old model of a mother staying at home with a baby was “no longer feasible.”²²³ He explained that holding on to that model was holding back the United States in making progress towards a realistic solution to the realities of working families.²²⁴ Almost twenty-five years later, it seems the Army is just starting to recognize this.

Dr. Brazelton explained that parents who have to leave their baby too soon guard themselves against attaching to the baby.²²⁵ Instead of focusing on learning about their baby, they are focused on “adjusting to time demands, to schedules, and to lining up the necessary substitute care.”²²⁶ His conclusions also included the role of the fathers. Dr.

²²⁰ *PDLA H.R. Hearing*, *supra* note 7, at 47 (statement of Dr. Berry Brazelton, Clinical Professor, Harvard Medical School and Professor of Psychiatry and Human Development, Brown University).

²²¹ Dr. Berry Brazelton graduated in 1943 from Columbia University College of Physicians and Surgeons in New York City. He conducted his pediatric training at Children’s Hospital in Boston and child psychiatry training at Massachusetts General Hospital. He established the Child Development Unit, a pediatric training and research center, at Children’s Hospital in 1972. Dr. Brazelton has published more than two hundred scientific papers and chapters. He developed and published the Neonatal Behavioral Assessment Scale used to assess physical, neurological, and emotional well-being of newborns. He is a Clinical Professor at Harvard Medical School and Professor of Psychiatry and Human Development at Brown University. Brazelton-Institute, <http://brazelton-institute.com/berrybio.html> (last visited Mar. 16, 2009).

²²² *See, e.g., PDLA H.R. Hearing*, *supra* note 7 (statement of Dr. Berry Brazelton, Clinical Professor, Harvard Medical School and Professor of Psychiatry and Human Development, Brown University); *Family and Medical Leave Act of 1991: Hearing on S. 5 Before the Comm. on Labor and Human Resources*, 102d Cong. 18–34 (1991) [hereinafter *Brazelton Testimony*]. In addition to these hearings, Dr. Brazelton testified at several other hearings during that time frame.

²²³ *PDLA H.R. Hearing*, *supra* note 7, at 48 (statement of Dr. Berry Brazelton, Clinical Professor, Harvard Medical School and Professor of Psychiatry and Human Development, Brown University). Active component female servicemembers have never “stayed home” and have faced the challenges Dr. Brazelton refers to since 1974. And since 1993, active component servicemembers have received six weeks less than their civilian counterparts.

²²⁴ *Id.*

²²⁵ *Id.* at 49.

²²⁶ *Id.* at 54.

Brazelton mentioned how “having the father involved in labor and delivery and present at the birth of the baby has significantly increased his sense of himself as a person who is important to his baby and to his mate.”²²⁷ Studies have also shown that paternal involvement with a newborn empowers a father to better understand his baby and to better support his wife.²²⁸ Dr. Brazelton explains the difficulties in establishing a necessary parent-infant bond:

The initial adjustment to the new baby at home is likely to be extremely stressful to any set of new parents. Most first-time parents have had little or no prior experience with babies or with their own parents as they nurtured a smaller sibling. They come to this new role without enough knowledge or participational experience. The generation gap makes it difficult for them to turn back to parents or extended family for support. Professional support is expensive and difficult to locate. The mother (and father) is likely to be physically exhausted and emotionally depressed for a period after delivery. The baby is unpredictable and has not developed a reliable day-night cycle of states of sleep and waking. Crying at the end of the day often serves as a necessary outlet and discharge for a small baby’s nervous system after an exciting but overwhelming day. This crying can easily be perceived as a sign of failure in parenting by harassed, inexperienced parents, and the crying that starts as a fussy period is then likely to become a colicky, inconsolable period at the end of every day for the next 3 months. Any mother is bound to feel inadequate and helpless at this time. She may wish to run away and to turn over her baby’s care to a “more competent person.” If she must go back to work in the midst of this trying period, it seems to me that she will never develop the same sense of understanding her baby and feeling competent to him or her as she might have if she’d been able to stay at home and to “see it out.”²²⁹

²²⁷ *Id.*

²²⁸ *Id.*

²²⁹ *Id.* at 54.

Dr. Brazelton also testified extensively on the four levels of behavioral organization in the communication system between parents and their small infants over the first four months.²³⁰ During this time, parents provide “affective and cognitive information and form the base for the infant’s learning about the world.”²³¹ “These early experiences of learning about each other are the base for their shared emotional development in the future, and are critical as anlagen for the infant’s future ego.”²³² Dr. Brazelton further explains, “When parents are deprived too early of this opportunity to participate in the baby’s developing ego structure, they lose the opportunity to understand the baby intimately and to feel their own role in development of these four stages.”²³³

Dr. Brazelton further described the loss a mother feels when she must share her small baby with a secondary caregiver.

Her feelings of competition with the other caregiver may well be uppermost in her consciousness. But underneath this conscious feeling of competition is likely to be a less-than-conscious sense of grief. Lindeman described a syndrome which he labeled a grief reaction, which seems to fit the experiences which mothers of small babies describe when they leave them in substitute care. They are apt to feel sad, helpless, hopeless, inadequate to their babies. They feel a sense of loneliness, of depression, of slowed down physical responses, and even of somatic symptoms. To protect themselves from these feelings, they are likely to develop three defenses. These are healthy, normal and necessary defenses, but they can interfere with the mother’s attachment to her baby if they are not properly evaluated. The younger the baby and the more inexperienced the mother, the stronger and more likely are these defenses. They are correlated with the earliness with which she returns to work.²³⁴

²³⁰ *Id.* at 56.

²³¹ *Id.*

²³² *Id.*

²³³ *Id.* at 61.

²³⁴ *Id.* at 61–62.

The three defenses to which Dr. Brazelton refers are denial, projection, and detachment. With denial, “[a] mother is likely to deny that her leaving matters—to either the child or to herself.”²³⁵ This may prevent a mother from being involved with the secondary care provider because it is too painful.²³⁶ Projection refers to a parent projecting the responsibilities of caregiving to the substitute caregivers.²³⁷ And finally, with detachment a mother has a tendency to “distance her feelings of responsibility and intense attachment.”²³⁸

The military has recently made two changes that seem to exhibit its own better understanding of the importance of parent-infant bonding. First, Congress, upon a request from the military, recently passed a law granting ten days paternity leave following the birth of a child to allow a father more time to spend with the child and his wife.²³⁹ The main proponent of this law was the Navy, which was supported by the other services.²⁴⁰ Secondly, the Army and Air Force recently extended its postpartum deployment deferral from four months to six months.²⁴¹ This additional time was advocated for the main purpose of allowing mothers more time to bond with their infants.²⁴²

The Army should increase the length of time for paternity leave. Fathers are an important part of the bonding process. One study found, “Fathers and their efforts are important for the development of the newborn child and family.”²⁴³ In this study, all the men took two to four months of parental leave.²⁴⁴ The men reported that spending time alone with the child and learning to care for the child without the mother present was empowering.²⁴⁵ Additionally, it is difficult for a father who

²³⁵ *Id.* at 62.

²³⁶ *Id.*

²³⁷ *Id.*

²³⁸ *Id.*

²³⁹ 10 U.S.C.S. § 701(j)(1)–(2) (LexisNexis 2008), amended by NDAA 2009, Pub. L. No. 110-417, 122 Stat. 4356, 4449 (2008).

²⁴⁰ Clark Telephone Interview, *supra* note 119.

²⁴¹ Postpartum Deferment Policy Change, *supra* note 79.

²⁴² Neilsen Telephone Interview, *supra* note 108. Colonel Nielsen explained he strongly advocated for one year but was not supported due to mission requirements. He also explained the breastfeeding rationale was not addressed because of questions concerning how to apply the policy to females who did not breastfeed.

²⁴³ Asa Premberg et al., *Experiences of the First Year as Father*, 22 SCAND. J. CARING SCI. 56, 56 (2008).

²⁴⁴ *Id.* at 56.

²⁴⁵ *Id.* at 57.

does not take parental leave to develop the same skills in caring for his newborn that his wife develops. This “marginalizes” his role as a caregiver and “plac[es] the predominant burden on the mother.”²⁴⁶ Although the recent implementation of paternity leave is a positive step for members of the armed forces, ten days does not provide enough time for the bonding process advocated above.

D. Better Performance of Servicemember

Increasing postpartum leave will improve the work performance of postpartum parents for several reasons. First, the mother will be more rested and more physically and mentally prepared to perform her military duties. Expecting new mothers to return to work at six weeks postpartum in a more fatigued state than their peers could lead to an increased risk for injury and at a minimum, less efficient performance. By way of example, one of the strongest proponents of parental leave was the United Mine Workers of America Association.²⁴⁷ The Association found that longer parental leave resulted in its employees being less fatigued at work, which resulted in fewer accidents.²⁴⁸ The spokesman testified, “We believe that any additional cost of the Parental Leave Program would be minimal and offset by cost savings due to the reduction of stress-related accidents.”²⁴⁹

Second, when both parents work outside the home, their child’s illness is often a reason for missing work.²⁵⁰ Preschool children often have to stay home from daycare centers due to common side effects of exposure to other children with illnesses, to include fevers and diarrhea (both symptoms exclude children from childcare centers for at least twenty-four hours). Parents will miss less work because longer postpartum leave will enable an infant more time to build its immune system and to breastfeed, resulting in less illnesses and less absences for the parents. Although the unit would be without the servicemember for an additional six weeks, the extended leave would benefit the unit and the Army in the long run.

²⁴⁶ Martin H. Malin, *Fathers and Parental Leave*, 72 TEX. L. REV. 1047, 1057 (1994).

²⁴⁷ PDLA H.R. Hearing, *supra* note 7, at 82 (statement of Dr. Stephen F. Webber, International Executive Board Member of the United Mine Workers).

²⁴⁸ *Id.* at 81.

²⁴⁹ *Id.* at 82.

²⁵⁰ Cohen et al., *supra* note 196, at 149.

E. Improved Retention Rates

1. *Officer Attrition*²⁵¹

In FY 2007, the Army had 3000 fewer officers than required, with the most severe shortages being senior captains and majors with eleven to seventeen years of experience.²⁵² The Army expected the shortage to increase in FY 2008 to 3700.²⁵³ Retention rates for U.S. Army female servicemembers are lower than their male counterparts.²⁵⁴ As of 2008, females in the Army made up 16.9% of the officer corps, and 13.4% of the enlisted corps.²⁵⁵ In 2006, the retention rate for U.S. Army male captains was 89.96%, compared with only 85.81% for female captains.²⁵⁶ For majors, the retention rate for males was 93.10% versus only 90.87% for females.²⁵⁷ “Female military doctors, lawyers and chaplains are more likely than their male counterparts to leave the military after serving five to eight years.”²⁵⁸ After a successful company command at the eight-year mark, an active component female officer begins to consider remaining in the military for a full career; however, the desire to raise children becomes a reality.²⁵⁹ The Army’s shortage of mid-grade officers demands the Army pay special attention to a female’s desire to leave the service to raise a family.

²⁵¹ Army enlisted females have much lower retention rates than their male counterparts. ANNUAL REPORT ON FEMALES, *infra* note 254, at 37–40. Across most enlisted ranks, the difference between male and female retention is even greater than in the officer corps. Because HRC has an office dedicated to examining issues surrounding officer retention, the underlying data for this article was more accessible for officers than for the enlisted ranks.

²⁵² Colonel Samuel T. Piper III, Improving Retention Under the U.S. Army’s Captain Incentive Program 3 (Mar. 15, 2008) (unpublished Master of Strategic Studies Degree Research Paper, U.S. Army War College) (on file with author).

²⁵³ *Id.* at 3.

²⁵⁴ DEF. DATA MANPOWER CTR. & SERVS.’ HUMAN RES. STAFFS & COMMANDS, ANNUAL REPORT ON STATUS OF FEMALE MEMBERS OF THE ARMED FORCES OF THE UNITED STATES, FY2002–06, at 41–44 (2007) [hereinafter ANNUAL REPORT ON FEMALES].

²⁵⁵ FY08 ARMY PROFILE, *supra* note 144.

²⁵⁶ ANNUAL REPORT ON FEMALES, *supra* note 254, at 42.

²⁵⁷ *Id.* at 43.

²⁵⁸ Steven Donald Smith, *Committee Examines Issue of Women Separating From Military*, AM. FORCES PRESS SERVS. NEWS ART., Aug 28, 2006, <http://www.defenselink.mil/news/NewsArticle.aspx?ID=612>.

²⁵⁹ Telephone Interview with Lieutenant Colonel Lindenmeyer, Officer Personnel Military Strength Task Force, U.S. Army Human Res. Command (Jan. 16, 2009) [hereinafter Lindenmeyer Telephone Interview].

A majority of officers, both male and female, state family reasons as one of the main reasons for leaving the service.²⁶⁰ There are two common scenarios affecting retention rates. The first scenario impacts female retention rates. Female officers are more likely than male officers to leave military service to start a family or to pursue employment more suited to raising young children.²⁶¹ The Defense Department Advisory Committee on Women in the Service found women often leave the military to start a family.²⁶² One study determined female graduates from the U.S. Military Academy are the most likely group of officers to leave the military after their first term.²⁶³

Jane Waldfogel, a sociologist, hypothesized in her study on the effect of children on women's wages "that women minimize 'work and family conflict' by shifting occupations or jobs, altering their place of work—that is, making changes that enhance their ability to retain control of their children's lives but also exact a price in terms of their own earnings trajectories."²⁶⁴ In the civilian sector, the Department of Labor statistics indicate "only about one-third of mothers have returned to full-time work

²⁶⁰ Smith, *supra* note 258 ("The main reasons women are getting out after five to eight years of service is to start a family.") (quoting Mary Nelson, Chairwoman of the Defense Department Advisory Committee on Women in the Services); Telephone Interview with Lieutenant Colonel Douglas Ingros, Leader Development Division, Chief of Officer Retention (Jan. 12, 2009) [hereinafter Ingros Telephone Interview]. Lieutenant Colonel Ingros explains the Army does not specifically request officers' reasons for leaving military service during the expiration of term of service (ETS) process. *Id.* However, he is familiar with reasons officers provide prior to separation, and one of the top three reasons stated is because of the officer's spouse. *Id.* Often, the spouse is also trying to maintain a career made difficult by multiple moves or because of the servicemember's multiple deployments. *Id.*; Telephone Interview with Major Emily Schiffer, Judge Advocate Gen.'s Corps, Plans & Operations Branch (Manpower & Budget) (Jan. 13, 2009) [hereinafter Schiffer Telephone Interview] (explaining almost every exit survey submitted with an unqualified resignation listed family reasons as a main reason for leaving military service); U.S. GOV'T ACCOUNTABILITY OFFICE, REPORT TO THE COMM. ON ARMED SERVS., HOUSE OF REPRESENTATIVES, MILITARY PERSONNEL, STRATEGIC PLAN NEEDED TO ADDRESS ARMY'S EMERGING OFFICER ACCESSION AND RETENTION CHALLENGES (2007) [hereinafter OFFICER ACCESSION AND RETENTION CHALLENGES REPORT].

²⁶¹ Smith, *supra* note 258; OFFICER ACCESSION AND RETENTION CHALLENGES REPORT, *supra* note 260.

²⁶² Smith, *supra* note 258.

²⁶³ Lindenmeyer Telephone Interview, *supra* note 259; OFFICER ACCESSION AND RETENTION CHALLENGES REPORT, *supra* note 260.

²⁶⁴ Suzanne M. Bianchi, *Maternal Employment and Time with Children: Dramatic Change or Surprising Continuity?*, 37.4 DEMOGRAPHY 401, 408 (2000) (citing J. Waldfogel, *The Effect of Children on Women's Wages*, 62 AM. SOC. REV. 209–17 (1997)).

six months after the birth of their first child.”²⁶⁵ This, in conjunction with the Army’s own statistics on women leaving military service, are factors the Department of Defense retention personnel should consider as dispositive of what females desire during child-bearing years. Our most talented officers have several more flexible employment options available to them than service in the military.

The second scenario impacts male retention rates and is referred to as “equality of service.”²⁶⁶ This describes the desire of servicemembers’ spouses to maintain their own careers and quality of life while supporting their spouses’ military career.²⁶⁷ A societal consequence of more spouses having careers is the need for mothers and fathers to share more equally in caring for the children, which has historically been an area dominated by the mother. Suzanne M. Bianchi’s study finds the following:

In 1965[,] the time fathers reported spending primarily on childcare was about one-quarter the mothers’ estimate of their time with children; this figure increased to 30% of mothers’ estimates if secondary childcare time was included. By 1998, fathers’ (primary) childcare time was 56% of mothers’ time, and 45% of mothers’ time when secondary childcare time was added. In 1965, fathers reported having children with them about half as often as did mothers. By 1998, fathers’ time with children was two-thirds that of mothers.²⁶⁸

U.S. Army retention policies should adequately reflect these societal conditions in its efforts to retain the Army’s most talented, mid-level servicemembers. Adjusting parental leave policies is one way to do this.

2. *Retention and the U.S. Army Menu of Incentives*

The Human Resources Command Retention Office examines and recommends policies to retain military officers. The retention office is currently examining a menu of incentive offerings to determine retention

²⁶⁵ *Id.* at 408.

²⁶⁶ Lindenmeyer Telephone Interview, *supra* note 259.

²⁶⁷ *Id.*

²⁶⁸ Bianchi, *supra* note 264, at 410–11.

models that allow decision makers to look at quality of life initiatives.²⁶⁹ Part of the study includes an analysis of what motivates different generations of officers. The generation the Army is currently focused on retaining is labeled the Millennial generation.²⁷⁰ The Millennial generation is especially focused on balancing life and work throughout their careers, as opposed to at the end of their careers.²⁷¹ The military must compete to both recruit and to retain military personnel. Because the military is a “closed society,” there is a much higher cost to replace a servicemember than to replace a civilian employee.²⁷² For these reasons, and in a greater effort to retain talented officers, the Army is looking closely at how to retain more officers.

The Army Officer Menu of Incentives Program ran from September 2007 through November 2008 in an effort to retain more mid-grade officers.²⁷³ Critical Skills Retention Bonuses were offered but “[were] not large enough to entice officers to take this incentive.”²⁷⁴ Only 68% signed up for the incentives, and the Army was expecting 80%.²⁷⁵ Furthermore, many believe that the Incentives Program was just a temporary fix and has “simply delayed an inevitable train wreck or exodus of junior officers which will now occur in 2011.”²⁷⁶ Therefore, “continuing the momentum purchased by the Menu of Incentives is the U.S. Army’s next logical step for an Officer Retention strategy.”²⁷⁷

²⁶⁹ Lindenmeyer Telephone Interview, *supra* note 259.

²⁷⁰ Lieutenant Colonel Vincent Lindenmeyer, Menu of Incentives Feedback Survey (Jan. 2009) (unpublished PowerPoint Presentation) (on file with author); *see generally* Piper, *supra* note 252.

²⁷¹ Lieutenant Stephanie Miller, Women’s Policy, U.S. Navy, Task Force Life Work (Jan. 2009) (unpublished PowerPoint Presentation) (on file with author) [hereinafter Miller Presentation]; Interview by Pat Galagan with Marcus Buckingham, Author and Authority on Discovering and Maximizing Your Strengths, location unknown (Aug. 2006) (discussing engaging and developing Millennials’ special strengths).

²⁷² JEC PAID FAMILY LEAVE, *supra* note 135, at 4 (determining lowering turnover rates can reduce costs significantly for employers. The average cost of turnover for an employer is about twenty-five percent of an employee’s salary. A good estimate of costs includes the costs to search for a new employee and also training costs). Those costs are significantly higher in the military.

²⁷³ Piper, *supra* note 252, at 3.

²⁷⁴ *Id.* at 6.

²⁷⁵ *Id.*

²⁷⁶ Lieutenant Colonel Vincent Lindenmeyer, Maintaining the Officer Retention Momentum Through Low-Cost Options (9 Feb. 2009) [hereinafter Officer Retention Info. Paper] (on file with author).

²⁷⁷ *Id.*

While “cash is king,” it should be the final resort. During this time of economic crisis and future lack of additional funding, the U.S. Army must now consider low cost options other than cash to maintain the same level of engagement and retention with this generation.²⁷⁸ A comprehensive and integrated strategy focused on engaging and retaining the millennial generation through additional low cost options is the next step to maintain the momentum of the recently closed \$440 million Menu of Incentive Program. When cash is used, an institution is not motivated to change its culture. In the low cost options arena, the Army’s culture must be willing to change.²⁷⁹

The JAG Corps is one example of an area where the Army is losing talent in its mid-level grades, and low cost options could make a difference. The JAG Corps recently conducted a survey of its servicemembers to determine what incentives might convince JAG officers to remain in the service for another tour of duty.²⁸⁰ Options considered were financial incentives, duty station of choice, job of choice, and a possible sabbatical. Financial incentives ranked the highest, and the sabbatical option ranked lower on the list.²⁸¹ Results were not separated by gender so it is not possible to determine if mostly females chose the sabbatical option.²⁸²

More dispositive of the desires of young female law associates is the practice of civilian law firms, which have found offering extensive maternity leave benefits is essential to recruiting the most qualified female attorneys.²⁸³ Considering 50% of law school graduates are female, it is easy to understand why this benefit is important to new associates. Additionally, 25.8% of JAG officers are female, almost 9% more than the overall percentage of females in the Army as a whole.²⁸⁴

²⁷⁸ *Id.*

²⁷⁹ *Id.*

²⁸⁰ U.S. ARMY JUDGE ADVOCATE GEN. PERS., PLANS & TRAINING OFFICE, OFFICER SURVEY ON RETENTION: ACTIVE AND RESERVES (2008).

²⁸¹ Schiffer Telephone Interview, *supra* note 260.

²⁸² *Id.* Mostly female officers use the Coast Guard sabbatical option. Interview with Lieutenant Commander Scott Herman, USCG, Senior Coastguardsmen, Ctr. for Law & Military Operations, TJAGLCS, Charlottesville, Va. (Mar. 5, 2009).

²⁸³ Associate Pirate, *supra* note 138.

²⁸⁴ E-mail from Jagman Singh, Office of the Judge Advocate Gen., to author (21 Jan. 2009 1045 EST) (on file with author). The Medical Corps also has a higher percentage

A more generous maternity leave policy in the Army would likely have a positive impact on recruiting and retaining mid-grade female judge advocates.

Based on parental leave policies offered by civilian corporations, the statements of servicemembers who have left the service for family reasons, and the Navy's recent surveys conducted of its fleet,²⁸⁵ it is likely the Army could increase the retention of mid-level officers and enlisted members by providing better postpartum leave benefits. The retention of females is lower than for males.²⁸⁶ In a time where retention of talented servicemembers is a significant issue, and money for bonuses is limited, low cost options, such as better parental leave, should be given greater consideration. Furthermore, such consideration would also be in line with the Army's recent promise to provide more support to Army families through the implementation of the Army Family Covenant.

VI. Counterarguments

Opponents of extending postpartum leave have several counterarguments. This section addresses those arguments.

First, some may argue the military leave policy is better than the FMLA offered to civilians because the military provides paid leave. This is inaccurate. Many companies provide paid leave for their employees,²⁸⁷ and many civilians have the option to purchase short-term disability leave to compensate for any leave.²⁸⁸ Also, many states have laws supplementing income while on parental leave.²⁸⁹ Additionally, federal legislation providing paid leave has been introduced several times over the past few years and has been introduced again in 2009.²⁹⁰ It is only a matter of time before this legislation becomes law, especially under the current administration and Congressional composition. Soon,

of females than the rest of the Army, and it also struggles with retention. Nielsen Telephone Interview, *supra* note 108.

²⁸⁵ Miller Presentation, *supra* note 271.

²⁸⁶ ANNUAL REPORT ON FEMALES, *supra* note 254.

²⁸⁷ JEC PAID FAMILY LEAVE, *supra* note 135, at 4.

²⁸⁸ *Id.* at 12.

²⁸⁹ *Id.*

²⁹⁰ Federal Employees Paid Parental Leave Act, S. 354, 111th Cong. (2009); H.R. 626, 111th Cong. (2009).

the military will be even further behind societal norms in the parental leave benefits it offers its servicemembers.

Second, in countering improved health benefits to infants, opponents might argue that (1) improving the quality of daycare centers eliminates the risk of exposure to viruses or bacteria, and (2) having more illnesses as infants builds immune systems and leads to fewer illnesses when they reach school-age.

Improving the quality of daycare centers would not be enough to improve infant health. Most homes are more sterile than daycare facilities because large numbers of other children are not present and exposure to germs is, therefore, limited. Additionally, not all children can be admitted into the military Child Development Centers, or parents may opt to take their infant somewhere less expensive. For example, the Fort Myer, Virginia, Child Development Center opened in June 2008 and currently has a one-year waiting list for all preschool-aged children.²⁹¹

Additionally, the argument that being ill as an infant helps build the immune system and leads to fewer illnesses as a school-age child ignores the health benefits of breastfeeding, which is easier to provide when the mother is afforded adequate time to establish breastfeeding.²⁹² This argument also ignores the disruption caused by the numerous illnesses the infant and parent must suffer prior to the child reaching school-age, and it does not consider that the infant actually has to survive to reach school-age children.

Third, opponents may argue that providing maternity leave to female servicemembers for reasons other than to convalesce would violate the Equal Protection Clause of the U.S. Constitution because it would not afford the same benefits to male servicemembers. First, male servicemembers are now entitled to paternity leave.²⁹³ Second, biological differences between males and females, to include the female's exclusive ability to breastfeed, must be acknowledged. Additionally, these same biological differences cause discrimination against women and prevent them from serving in various positions in the

²⁹¹ Telephone Interview with Patty Sanders, Dir. of Cent. Enrollment, Fort Myer, Virginia Child Dev. Ctr., Fort Myer, Va. (Mar. 10, 2009).

²⁹² Ball et al., *supra* note 172, at 154.

²⁹³ 10 U.S.C.S. § 701(j)(1)–(2) (LexisNexis 2008), *amended by* NDAA 2009, Pub. L. No. 110-417, 122 Stat. 4356, 4449 (2008).

military.²⁹⁴ This discrimination is considered acceptable in the military with courts giving great deference to the military in its determinations of what is necessary to accomplish its mission.²⁹⁵ The law would give the Army similar discretion in applying its parental leave policies for the same reasons.

The Army's primary mission is to serve the national interest and to fight and win our nations wars. To accomplish this mission, the Army can and does discriminate between males and females.²⁹⁶ Females are not allowed to serve in various specialties and positions, and openly homosexual individuals are not allowed to serve at all. Similarly, if it is determined that the Army could not accomplish its mission if male servicemembers were afforded the same parental leave as female servicemembers, the Army would be given the discretion to afford such benefits only to females. This would be justified by a female's biological and exclusive ability to breastfeed, and the reality that mission accomplishment would be affected much more by the absence of both female and male servicemembers for twelve-week intervals. Therefore, females should be afforded the opportunity to take the leave even if it cannot be afforded to both sexes.

Also, the Army's diversity policy should embrace and accept the differences that nature cannot change, and regulate accordingly. If one of the reasons stated for the extended leave is the establishment and maintenance of breastfeeding, the equal opportunity argument loses strength. Statistics show that more female servicemembers will breastfeed if given more postpartum leave.²⁹⁷

Fourth, opponents to extending postpartum leave may argue it will degrade mission accomplishment in various ways. Foremost, female servicemembers are not deployable for six months after childbirth, so

²⁹⁴ National Defense Authorization Act for Fiscal Year 1994, Pub. L. No. 103-160, § 542, 107 Stat. 1547, 1659 (1993), as amended by Pub. L. No. 106-398, 114 Stat. 1654 (2000) and Pub. L. No. 107-107, 115 Stat. 1125 (2001).

²⁹⁵ See, e.g., *Parker v. Levy*, 417 U.S. 733, 758-59 (1975); *Schlesinger v. Councilmen*, 420 U.S. 738, 757 (1975).

²⁹⁶ See, e.g., § 542, 107 Stat. at 1547; U.S. DEP'T OF ARMY, REG. 635-200, ACTIVE DUTY ENLISTED ADMINISTRATIVE SEPARATIONS para. 15-2 (6 June 2005) (explaining homosexual conduct is grounds for separation); U.S. DEP'T OF ARMY, REG. 600-20, ARMY COMMAND POLICY (11 Feb. 2009) (providing guidance to military commanders on maintaining well-being of the force); Military Selective Service Act, 50 U.S.C. App. 451-473 (2000) (requiring only males to register).

²⁹⁷ Calnen, *supra* note 153, at 39.

extending postpartum leave to twelve weeks will not interfere with deployments. Next, opponents may argue that increasing postpartum leave will incentivize childbirth in the military, further degrading mission accomplishment. There are three problems with this argument. First, does that counterargument mean the Army will not consider providing what is best for a new mother and her infant in order to discourage women in the military from having children? Second, fertility rates have actually dropped in the United States²⁹⁸ and pregnancy rates of female servicemembers are likely the same or lower than the national average.²⁹⁹ At any given time, only ten percent of all active component females are pregnant.³⁰⁰ Third, it seems unlikely that female servicemembers will make a lifelong commitment to raise a child simply to obtain a few extra weeks of leave.

Although extending parental leave might temporarily affect mission accomplishment, the argument cannot stop there. Overall, improving such policies will benefit the Army organization and improve mission accomplishment by improving servicemember performance and reducing attrition. As mentioned in Part IV.A, 59% of all women work and 71% of working women have children under the under the age of eighteen.³⁰¹ Sixteen percent have children under the age of six.³⁰² “In 2007, women accounted for about 51% of all persons employed in management, professional, and related occupations”³⁰³ Women are going to work, but the question is where? It is up to the Department of Defense to decide if they want to recruit and retain working women, or whether they want them to work somewhere other than the military. The Army should consider a culture change in the way it thinks about providing for new mothers and newborn dependents if it wants to maintain more of its most talented mid-level female servicemembers. If the Army is truly committed to its military families as the Army Family Covenant states, it should give serious consideration to modifying its postpartum policies.³⁰⁴

²⁹⁸ U.S. CENSUS BUREAU, REPORT ON U.S. FERTILITY RATES (2008).

²⁹⁹ The author believes current operational tempo has delayed many female servicemembers from starting families.

³⁰⁰ Nielsen Telephone Interview, *supra* note 108.

³⁰¹ HOUSEHOLD DATA ANNUAL AVERAGES, *supra* note 133.

³⁰² *Id.*

³⁰³ U.S. BUREAU OF LABOR SERVICES, WOMEN IN THE LABOR FORCE: A DATABOOK 1 (Dec. 2008).

³⁰⁴ The author believes the Army is not making this culture change. Instead of increasing the hours of the Child Development Centers on posts as has been touted as an accomplishment under the new Army Family Covenant, the Army should be looking at

Opponents may argue the Army should not expend much effort on retaining females, especially if it means offering an additional six weeks of postpartum leave following childbirth. Such opponents might argue those positions could then be filled with males. That argument would overlook the challenges of maintaining an all volunteer military and the reason women were fully integrated into the military in the first place.³⁰⁵ As of September 30, 2008, the overall strength of women in the Army was 13.58%.³⁰⁶ Most of the females are between the ages of twenty and thirty-eight,³⁰⁷ the medically best ages to bear children.³⁰⁸ The reality is that only 10% of those 13.58% will be pregnant at any time.³⁰⁹ When the Army eliminated the Women's Army Corps and integrated females into the regular Army in 1978,³¹⁰ the Army committed to the reality that female servicemembers would bear children during their time in service.

Furthermore, suggesting the Army eliminate or reduce the number of women in the military would overlook the qualities and diversity females add to the military. One of the Army's goals is to have a diverse force. Department of the Army Pamphlet 350-20, Unit Equal Opportunity Training, defines diversity as "[a] way of creating an environment that will enable all people to reach their full potential in pursuing organizational objectives."³¹¹ It further explains that managing equal opportunity can be defined by enabling the "[f]ull use of one's potential regardless of race, color, religion, or national origin."³¹² There also needs to be a recognition that the organization will have to change its culture to create an environment to meet the needs of its Soldiers.³¹³

more ways to allow Soldiers to take care of their children rather than providing more hours for someone else to take care of them.

³⁰⁵ See generally *supra* Section III.A.1; MORDEN, *supra* note 81, at 257 (explaining the end of the draft required the need for women as a manpower resource).

³⁰⁶ FY08 ARMY PROFILE, *supra* note 144.

³⁰⁷ OFFICE OF ARMY DEMOGRAPHICS, FY08 AGE DISTRIBUTION FOR THE ACTIVE COMPONENT, BY GENDER AND RANK (2008) (on file with author).

³⁰⁸ Emma Dickinson, *Best Age for Childbearing Remains 20-35—Delaying Risks Heartbreak Says Experts*, MED. NEWS TODAY, Sept. 16, 2005, <http://www.medicalnewstoday.com/articles/30737.php>.

³⁰⁹ Neilsen Telephone Interview, *supra* note 108.

³¹⁰ MORDEN, *supra* note 81, at 397.

³¹¹ U.S. DEP'T OF ARMY, PAM. 350-20, UNIT EQUAL OPPORTUNITY TRAINING fig.9-2 (1 June 1994) [hereinafter DA PAM. 350-20].

³¹² *Id.* para. 9-3.

³¹³ *Id.* The training example used actually refers to retaining unmarried, pregnant Soldiers; years ago, they would have been separated.

The Army has embraced females in the service. General MacArthur called the Women's Army Corps Soldiers "my best soldiers," adding that "they worked harder, complained less, and were better disciplined than men."³¹⁴ The chairwoman of the Defense Department Advisory on Women in the Services (DACOWITS) stated in an article about retaining women in the military,

Numerous high-ranking military officials of both genders stressed . . . that women offer something the military would not have without them. They offer a different perspective. They offer a different way of looking at things, a different way of communicating, a different way of gathering points of view and getting consensus. It's a different way of doing things, and it's something the military members I've talked to feel very strongly that the military needs.³¹⁵

Striving for a diverse military force should be embraced to make the strength of the whole stronger. Therefore, women should continue to serve despite the necessity to occasionally accommodate the biological reality of childbearing.

VII. Proposal

The portions of the FMLA that should be extended to servicemembers include modified versions of maternity leave and paternity leave. Postpartum leave should be extended to twelve weeks for female servicemembers and four weeks for male servicemembers. For females, six weeks should be allocated for recovery from childbirth, and six weeks should be designated for bonding with the infant, adjusting to parenthood, and facilitating breastfeeding. Specifically allocating such intervals would give flexibility to servicemembers who deliver prematurely or whose infant spends a significant amount of time in the hospital before returning home. Providing only four weeks for males, as opposed to the twelve weeks they would receive as civilians, realistically addresses the mission requirements of the Army. Male servicemembers

³¹⁴ Melissa K. Wilford, *Army Observes 30th Anniversary of Integrating WACs*, Oct. 20, 2008, <http://www.army.mil/-news/2008/10/20/13428-army-observes-30th-anniversary-of-integration>.

³¹⁵ Smith, *supra* note 258.

should be able to take the four weeks at any time during the sixteen weeks following the birth. This would allow the unit flexibility, and it would also allow the parents to elect to keep the infant at home for a maximum of sixteen weeks should the father opt to take his paternity leave after the mother takes her maternity leave. If the Army is really going to care for its families, it must let the father play a larger role in his own family. Four weeks is a small accommodation in an effort to make the military a more appealing place to spend a career.

The entire postpartum leave period should be paid. Too many eligible employees cannot take full advantage of FMLA benefits because it is unpaid. To make the Army maternity policy realistic, and to make it available regardless of pay grade, maternity leave must be paid. Furthermore, several civilian companies offer paid maternity leave benefits, and the Army must do the same to recruit and retain the most talented servicemembers.

In the alternative, servicemembers should be given the option of taking an additional six weeks of leave beyond the currently provided six weeks of convalescent leave, and the six weeks should be added to their active duty service obligation.³¹⁶ This would only apply if the military continued to pay the servicemember while on leave; otherwise, the active duty service obligation would remain the same.

One final recommendation is to allow servicemembers to take a one-year unpaid sabbatical in addition to postpartum leave.³¹⁷ Should units have difficulty filling certain critical positions during the period of absence, reservists should be considered to serve as temporary replacements during this time period.

³¹⁶ Although longer active duty service obligation (ADSO) periods were considered, the author believes caring for an infant is not the same type of benefit to a Soldier as, for example, earning a civilian degree, which normally increases a Soldier's ADSO by two years for every one year of education. Rather, the benefit is to the infant and the Army, and postpartum leave should be a right provided to a new mother. See U.S. DEP'T OF ARMY, REG. 350-100, OFFICER ACTIVE DUTY OBLIGATIONS (8 Aug. 2007) [hereinafter AR 350-100].

³¹⁷ The 2009 NDAA allocated each service twenty slots to pilot a sabbatical program. NDAA 2009, Pub. L. No. 110-417, 122 Stat. 4356, 4449 (2008). The implementation may not occur for approximately two years because of legal and administrative details. Lindenmeyer Telephone Interview, *supra* note 259. Additionally, the Coast Guard provides its officers the option for a two-year sabbatical. COMDSTINST M1000.6A, *supra* note 79.

This proposal is supported by the five reasons discussed above. First, longer postpartum leave will lead to the improved health of the infant. The FMLA provides twelve weeks of maternity leave to male and female employees following the birth of a child. Although advocates fought for even more, twelve weeks was determined to be the absolute minimum reasonable time for the health of the baby and for bonding. A female's choice to serve in the military as opposed to the civilian work force should not deny her newborn child the same health standards Congress has determined are required for infants of civilian parents.

Second, in addition to improving infant health, increased postpartum leave will improve parent health. As infants begin to sleep for longer periods of time during the night, mothers will also benefit from greater sleep intervals. Also, studies show women's mental and emotional health improves with longer periods of maternity leave.³¹⁸

Third, the length of postpartum leave for servicemembers should be extended to improve the quality of bonding between the infant and the mother. Military service demands much time from its members, often at the expense of time away from immediate family members. Long duty days including morning physical training, overnight training exercises, and deployments cause military parents to miss much of their children's lives. As this article explained, the first few months in an infant's life are essential in establishing a foundation of communications and intimacy between parents and a child.³¹⁹ It is also during this time that parents become secure in their role as nurturers for their child.³²⁰ This is especially true for mothers. This bond is difficult to secure in six short weeks before returning to twelve-hour duty days. Developing a policy regarding "maternity" leave that includes more adequate time to bond, in conjunction with convalescent leave, would alleviate some of this problem.

Fourth, improvements in all of the above-stated areas will improve servicemembers' overall performance. Better infant health will result in less parental absences from work to care for a sick child. Additionally, mothers would be more rested and mentally prepared to balance motherhood and childcare responsibilities.

³¹⁸ Baker et al., *supra* note 149, at 874.

³¹⁹ Brazelton Testimony, *supra* note 222.

³²⁰ *Id.*

Finally, expanding parental and family benefits to servicemembers can contribute to an overall effort to provide low-cost options to increase long-term retention of our most talented and experienced Soldiers. Each time a Soldier leaves the military, the military incurs the costs, time, and risks associated with training another Soldier to take his or her place.³²¹ Unlike civilian corporations, the Army only promotes from within. Because many Soldiers cite family as a significant reason for leaving the military,³²² expanding the Army's leave policy to include portions consistent with the FMLA would have a positive long-term effect on retention and morale.

VIII. Conclusion

The time has come for Congress to expand military leave entitlements³²³ to include provisions similar to those provided by the FMLA. The Army needs a better parental leave policy.³²⁴ This article proposes Congress amend 10 U.S.C. § 701 to entitle active component female servicemembers twelve weeks maternity leave following the birth of a child, active component male servicemembers four weeks paternity leave following the birth of a child, and male and female servicemembers six weeks following the adoption of a child. This would provide benefits more consistent with the FMLA, current state laws, international policy, and the Army's own renewed commitment to families.³²⁵

In 1978, when women were first allowed to remain in military service after becoming a parent, it could be said the Army was on the "cutting edge." It was one of the few places of employment that offered job protection and benefits by granting female servicemembers paid

³²¹ Ingros Telephone Interview, *supra* note 260.

³²² Smith, *supra* note 258; Ingros Telephone Interview, *supra* note 260; Schiffer Telephone Interview, *supra* note 260.

³²³ 10 U.S.C. § 701 (2006).

³²⁴ The Army does not appear concerned with adjusting its policies to retain female servicemembers. The Navy, on the other hand, has collected data on female servicemembers' concerns. Miller Presentation, *supra* note 271. In addition to data stating 45% of Sailors leave the service because of children, the Navy has found 16% believe better pregnancy support is important, and 12% believe better paternity leave is important. *Id.* Suggestions made from the fleet to the Task Force Life/Work included six weeks of maternity leave followed by four weeks of four hour days and having maternity leave match corporate America. *Id.* Fifty-eight percent of all college graduates are women, and this is talent that must be recruited and retained. *Id.*

³²⁵ See *Army Family Covenant*, *supra* note 2.

convalescent leave after childbirth. However, the Army has failed to revisit its policy on postpartum leave since that time.³²⁶ The rest of American society, to include Congress and private industry, as well as other industrialized nations, have examined the medical and social policy reasons to afford opportunities for parents to care for new infants while providing job protection, benefits, and pay following childbirth. It is time for the Army to do the same and truly acknowledge the role of Army families in today's military.

³²⁶ See sources cited *supra* note 108.

**DON'T ASK, DO TELL: THE IMPLICATIONS OF 2008
CIRCUIT COURT DECISIONS FOR THE STANDARD OF
CONSTITUTIONAL REVIEW APPLICABLE TO THE
MILITARY HOMOSEXUAL CONDUCT POLICY**

MAJOR BAILEY W. BROWN, III*

The laws involved . . . here are, to be sure, statutes that purport to do no more than prohibit a particular sexual act. Their penalties and purposes, though, have more far-reaching consequences, touching upon the most private human conduct, sexual behavior, and in the most private of places, the home.¹

I. Introduction

Gay and lesbian servicemembers have reason for cautious optimism.² Two recent federal circuit court decisions have confronted, with different results, significant questions surrounding the military's homosexual conduct policy, codified at 10 U.S.C. § 654³ and "colloquially known as 'Don't Ask, Don't Tell'" (DADT).⁴ As written, DADT requires

* Judge Advocate, U.S. Army. Presently assigned as the Deputy Staff Judge Advocate, U.S. Army Garrison, Fort McPherson, Ga. LL.M., 2009, The Judge Advocate Gen.'s Legal Ctr. & Sch., U.S. Army, Charlottesville, Va.; J.D., 2000, University of Georgia; B.A., 1997, The University of the South at Sewanee, Tenn. Previous assignments include Brigade Judge Advocate, 501st Sustainment Brigade, Daegu, Korea, 2006–2008; Brigade Judge Advocate, 18th Engineer Brigade (Theater Army), Bagram Afghanistan, 2005–2006; Chief, Personnel Claims, Europe, U.S. Army Europe and 7th Army, Mannheim, F.R.G., 2003–2005; Legal Assistance Attorney, U.S. Army Southern European Task Force (SETAF) (Airborne), Vicenza, Italy, 2001–2003. Member of the Georgia Bar. This article was submitted in partial completion of the Master of Laws requirements of the 57th Judge Advocate Officer Graduate Course.

¹ *Lawrence v. Texas*, 539 U.S. 558, 567 (2003).

² Optimism is warranted because, along with a changing national political climate, recent judicial scrutiny of the military policy against homosexual conduct casts doubt on its constitutionality. Caution is warranted because some scholars regard the political leanings of the Supreme Court bench as the critical factor for any judicially motivated change, with those on the left likely to strike the policy and those on the right more likely to support it; and those on the right have more votes in the end." E-mail from Shaun Martin, Law Professor, University of San Diego School of Law (Oct. 9, 2008, 14:09:31 EST) (on file with author).

³ 10 U.S.C. § 654 (2006) (concerning homosexuality in the armed forces).

⁴ *Thomasson v. Perry*, 80 F.3d 915, 920 (4th Cir. 1996).

separation of all military members who engage in homosexual acts.⁵ In *Witt v. Department of the Air Force (Witt)*,⁶ plaintiff Major Margaret Witt was suspended from reserve duties as an Air Force nurse pending separation proceedings under DADT.⁷ She had served eighteen years, was highly decorated⁸ and generally regarded as an outstanding officer, and was featured in Air Force promotional and recruiting materials for more than ten years, starting in 1993.⁹ From 1997 to 2003, Major Witt was involved in a committed same-sex relationship in which she and her partner lived together in a home 250 miles from the military base where she performed her reserve duties.¹⁰ In 2004, the Air Force commenced the investigation which led to the separation action.¹¹

She brought action in federal court to enjoin the Air Force from separating her.¹² In May 2008, the Ninth Circuit Court of Appeals determined that the Supreme Court decision in *Lawrence v. Texas (Lawrence)*¹³ requires the military to demonstrate that each specific servicemember's acts adversely impact the concerned military unit prior to separating the servicemember under DADT.¹⁴ *Witt* required consideration of each case on its own facts, precluding blanket application of the policy.¹⁵ To that end, the circuit court remanded the case to the district level, where the Air Force will have an opportunity to present evidence in satisfaction of this new requirement.¹⁶ As crushing a defeat as this decision was for DADT, the dissent demanded an even more stringent review, suggesting that the policy should be measured

⁵ 10 U.S.C. § 654(b)(1).

⁶ 527 F.3d 806 (2008).

⁷ *Id.* at 809.

⁸ *See id.* Major Witt's awards include "the Meritorious Service Medal, the Air Medal, the Aerial Achievement Medal, the Air Force Commendation Medal, and numerous others."

Id.

⁹ *Id.*

¹⁰ *Id.* ("Major Witt's partner was never a member nor a civilian employee of any branch of the armed forces, and Major Witt states that she never had sexual relations while on duty or while on the grounds of any Air Force base.").

¹¹ *Id.* at 810.

¹² *Id.*

¹³ 539 U.S. 558, 567 (2003).

¹⁴ *Witt*, 527 F.3d at 819.

¹⁵ *Id.*

¹⁶ *Id.* at 821.

against the strictest constitutional standard.¹⁷ The policy would not likely survive the dissent's proposed constitutional review.¹⁸

In June 2008, the First Circuit Court of Appeals in *Cook v. Gates* (*Cook*)¹⁹ confronted the identical issue. In this case, twelve former military members²⁰ who had been separated under DADT brought an action claiming that DADT is unconstitutional based upon due process, equal protection, and free speech grounds.²¹ The First Circuit agreed with *Witt* that the Supreme Court in *Lawrence* imposed "a standard of review that lies between strict scrutiny and rational basis,"²² but stated that, "[i]n *Witt*, the 9th Circuit resolved an as-applied, post-*Lawrence* substantive due process challenge to [DADT] differently than we do here."²³ In contrast to the *Witt* analysis, the First Circuit determined that DADT survived this higher level of constitutional scrutiny, even on a case-by-case basis, due to judicial deference to the legislature concerning military affairs.²⁴

As a result of these conflicting circuit court decisions, the Supreme Court of the United States may consider the military's ban on homosexual servicemembers ripe for constitutional review. Both these cases read *Lawrence* to require a heightened level of constitutional

¹⁷ *Id.* at 822 (Canby, J., dissenting) (arguing that DADT should be subject to strict scrutiny).

¹⁸ *Id.* at 817 (majority opinion) ("Few laws survive such scrutiny, and DADT most likely would not."); see also Pamela Lundquist, *Essential to the National Security: An Executive Ban on Don't Ask, Don't Tell*, 16 AM. U.J. GENDER SOC. POL'Y & L. 115, 124 (2007) (stating that courts applying strict scrutiny to DADT have found it unconstitutional, but that "those cases have been overturned on appeal," (citing *Watkins v. U.S. Army*, 837 F.2d 1428, 1451 (9th Cir. 1988) ("[T]he Army's regulations violate the constitutional guarantee of equal protection of the laws because they discriminate against persons of homosexual orientation, a suspect class, and because the regulations are not necessary to promote a legitimate compelling governmental interest."), *vacated*, 875 F.2d 699, 731 (9th Cir. 1989) (en banc), and *Able v. United States*, 968 F. Supp. 850, 864 (E.D.N.Y. 1997) (stating that "the Act discriminates against homosexuals in order to cater to the prejudices of heterosexuals"), *rev'd on appeal*, 155 F.3d 628, 635 (2d Cir. 1998))).

¹⁹ 528 F.3d 42 (2008).

²⁰ Details of each plaintiff can be found at the Service Member's Legal Defense Network website, <http://www.sldn.org/pages/plaintiffs-in-cook-v-gates> (last visited May 19, 2009).

²¹ *Cook*, 528 F.3d at 47.

²² *Id.* at 56.

²³ *Id.* at 48 n.10 (citing *Witt*, 527 F.3d. 806).

²⁴ *Id.* at 60.

scrutiny for DADT—a scrutiny it may not survive.²⁵ The differences in the analysis presented by the two circuits, as well as the disparate results in the two cases, invite an attempt by the highest Court to resolve this matter of contentious public and legal debate. This article predicts the result of such an attempt by examining the law surrounding DADT and the historical developments leading to the present debate. It closely examines the language and intent of the *Lawrence* decision and reviews the recent cases that have caused a split in the circuits about the standard of review established in *Lawrence*. It compares their treatment of the due process and equal protection arguments, and addresses the First Amendment arguments posed in *Cook*.

This article argues that the Supreme Court will do as the *Witt* and *Cook* courts have done and subject DADT to a higher than rational basis standard of review. The Court will not likely invalidate the policy under a strict scrutiny analysis. Instead, the policy will most likely survive in a weakened form requiring specific evidence of unit impact. From a practical standpoint, military judge advocates involved in the implementation of DADT should prepare to review files for evidence of adverse unit impact prior to separating personnel under DADT.

II. Background

A. Due Process

The Fourteenth Amendment states that “No State shall . . . deprive any person of life, liberty, or property, without due process of law.”²⁶ The Fifth Amendment states that no person “shall be deprived of life, liberty, or property without due process of law.”²⁷ While the due process analysis most often appears in the context of examining state statutes under the Fourteenth Amendment, courts apply the same analysis to

²⁵ See *Witt*, 527 F.3d at 827 (Canby, J., concurring in part and dissenting in part) (acknowledging that, under strict scrutiny analysis, “requiring the Air Force to make the requisite showing as a threshold matter may end the case”).

²⁶ U.S. CONST. amend. XIV § 1. The Supreme Court has long read the Fourteenth Amendment to incorporate the principles of the Bill of Rights and apply them to the states. See *Gitlow v. New York*, 268 U.S. 652 (1925) (“[F]reedom of speech and of the press—which are protected by the First Amendment from abridgment by Congress—are among the fundamental personal rights and ‘liberties’ protected by the due process clause of the Fourteenth Amendment from impairment by the States.”).

²⁷ U.S. CONST. amend. V.

legislation arising from the U.S. Congress under the Fifth Amendment.²⁸ The Supreme Court has read the due process language of these amendments to limit the ability of states or the Federal Government to intrude upon fundamental liberties without a proper basis,²⁹ “regardless of the procedures provided.”³⁰ Due process includes respect not only for liberties specifically enumerated in the Constitution, but also those “necessary in making the express guarantees fully meaningful.”³¹ Historically, the term liberty in the Fourteenth Amendment

denotes not merely freedom from bodily restraint but also the right of the individual to contract, to engage in any of the common occupations of life, to acquire useful knowledge, to marry, establish a home and bring up children, to worship God according to the dictates of his

²⁸ See *Troxel v. Granville*, 530 U.S. 57, 65 (2000), stating that:

The Fourteenth Amendment provides that no State shall “deprive any person of life, liberty, or property, without due process of law.” We have long recognized that the [Fourteenth] Amendment’s Due Process Clause, like its Fifth Amendment counterpart, “guarantees more than fair process.” The Clause also includes a substantive component that “provides heightened protection against government interference with certain fundamental rights and liberty interests.”

²⁹ See generally *Schwabe v. Bd. of Bar Examiners of N.M.*, 353 U.S. 232 (1957) (holding that due process requires the state to consider the individual circumstances of persons adversely affected by the application of a law).

³⁰ Brief of Appellee-Respondent at 33, *Witt v. Dep’t of the Air Force*, No. 06-35644 (9th Cir. Jan. 3, 2007).

³¹ *Griswold v. Connecticut*, 381 U.S. 479, 484 (1965). In *THE FEDERALIST*, NO. 84 (Alexander Hamilton), Hamilton argued that the naming of specific liberties should be unnecessary under the Constitution because the document itself limits the Government to its enumerated powers—none other should be available to it. He cautioned that “bills of rights are, in their origin, stipulations between kings and their subjects, abridgements of prerogative in favor of privilege, reservations of rights not surrendered to the prince,” *id.* at 578–79, and argued against enumerated liberties lest they become

exceptions to powers which are not granted; and on this very account, would afford a colourable pretext to claim more than were granted. For why declare that things shall not be done which there is no power to do? Why for instance, should it be said, that the liberty of the press shall not be restrained, when no power is given by which restrictions may be imposed? I will not contend that such a provision would confer a regulating power; but it is evident that it would furnish, to men disposed to usurp, a plausible pretence for claiming that power.

own conscience, and generally to enjoy those privileges long recognized at common law as essential to the orderly pursuit of happiness by free men . . . [t]his liberty may not be interfered with, under the guise of protecting the public interest, by legislative action which is arbitrary or without reasonable relation to some purpose within the competency of the State to effect. Determination by the legislature of what constitutes proper exercise of police power is not final or conclusive but is subject to supervision by the courts.³²

In the specific context of DADT, “the due process claim . . . is premised on the constitutional protection afforded all citizens to engage in certain sexual conduct,”³³ and challenges whether DADT intrudes upon “a realm of personal liberty which the government may not enter.”³⁴

B. Equal Protection

The Fourteenth Amendment also guarantees all citizens equal protection under the law.³⁵ Although the “inherent content of equal protection continues to be a subject of intense debate,”³⁶ the Supreme Court has interpreted this provision to mean that “[c]entral both to the idea of the rule of law and to our own Constitution’s guarantee of equal protection is the principle that government and each of its parts remain open on impartial terms to all who seek its assistance.”³⁷ Courts ordinarily find legislation compliant with equal protection principles so long as it “neither burdens a fundamental right, nor targets a suspect class . . . [and] bears a rational relation to some legitimate end.”³⁸

Id.

³² *Meyer v. Nebraska*, 262 U.S. 390, 399–400 (1923).

³³ *Cook v. Gates*, 528 F.3d 42, 60 (2008).

³⁴ *Lawrence v. Texas*, 539 U.S. 558, 579 (2003).

³⁵ U.S. CONST. amend. XIV. The Supreme “Court’s approach to Fifth Amendment equal protection claims has always been precisely the same as to equal protection claims under the Fourteenth Amendment.” *Weinberger v. Wiessenfeld*, 420 U.S. 636, 638 n.2 (1975).

³⁶ GERALD GUNTHER & KATHLEEN M. SULLIVAN, *CONSTITUTIONAL LAW* 628 (13th ed. 1997) (“[T]he strongest consensus about the meaning of equal protection is drawn from its historical origins: at the very least it was directed at governmental racial discrimination against blacks.”).

³⁷ *Romer v. Evans*, 517 U.S. 620, 633 (1996) (quoting *Sweatt v. Painter*, 339 U.S. 629, 635 (1950)).

³⁸ *Id.* at 631.

Neither the states nor the Federal Government³⁹ may indulge in “indiscriminate imposition of inequalities,”⁴⁰ and “certain interests, though not constitutionally guaranteed, must be accorded a special place in equal protection analysis.”⁴¹ In the specific context of DADT, “the equal protection claim is based on [DADT]’s differential treatment of homosexual military members versus heterosexual military members,”⁴² and challenges whether “homosexuals [are] a suspect class for equal protection purposes.”⁴³

C. Standards of Review in Constitutional Analysis

The Supreme Court has the power to strike down laws that violate constitutional principles pursuant to its power of judicial review.⁴⁴ Key to the fate of DADT is the standard of constitutional scrutiny the Supreme Court would apply in a potential judicial review of the statute.⁴⁵ There are three primary standards by which the Supreme Court examines a statute.⁴⁶ The rational basis test and the strict scrutiny test are considered the traditional standards,⁴⁷ having evolved over “a series of Supreme Court cases that have interpreted the Due Process and Equal Protection Clauses of the Fourteenth Amendment.”⁴⁸ Rational basis review examines “whether governmental action is so arbitrary that a rational basis for the action cannot even be conceived *post hoc*.”⁴⁹

³⁹ The process of incorporating the Fourteenth Amendment into the Fifth Amendment began with *Bolling v. Sharpe*; the Court explained that where the Fourteenth Amendment prevented states from segregating schools, “it would be unthinkable that the same Constitution would impose a lesser duty on the Federal Government.” 347 U.S. 497, 500 (1954).

⁴⁰ *Romer*, 517 U.S. at 633.

⁴¹ *Plyer v. Doe*, 457 U.S. 202, 233 (1982) (Blackman, J., concurring).

⁴² *Cook v. Gates*, 528 F.3d 42, 60 (2008).

⁴³ *Id.* at 51.

⁴⁴ See generally *Marbury v. Madison*, 5 U.S. (1 Cranch) 137 (1803).

⁴⁵ See generally *Lochner v. New York*, 198 U.S. 45 (1905). Justice Oliver Wendell Holmes’ informative dissent provides a general discussion of judicial review standards. *Id.* at 74.

⁴⁶ See Pamela Glazner, *Constitutional Law Doctrine Meets Reality: Don’t Ask, Don’t Tell in Light of Lawrence v. Texas*, 46 SANTA CLARA L. REV. 635, 639 (2003) (pithily explaining that “strict scrutiny sits atop intermediate scrutiny, which sits atop rational basis review”).

⁴⁷ *Witt v. Dep’t of the Air Force*, 527 F.3d 806, 818 (2008) (“Substantive due process cases typically apply strict scrutiny in the case of a fundamental right and rational basis review in all other cases.”); see also Glazner, *supra* note 46, at 640.

⁴⁸ Glazner, *supra* note 46, at 640.

⁴⁹ *Witt*, 527 F.3d at 817.

Critically, this standard of review “does not permit consideration of the strength of the individual’s interest or the extent of the intrusion on that interest caused by the law; the focus is entirely on the rationality of the state’s reason for enacting the law.”⁵⁰ A law will survive the rational basis test so long as the law in question is rationally related to a legitimate government interest, and its objectives are not “themselves invalid.”⁵¹

The second traditional standard, strict scrutiny, is often the death knell of the subject legislation.⁵² Legislation “infringing on fundamental rights receives strict scrutiny, which requires the government to establish that the means the law employs ‘are suitably [or “narrowly”⁵³] tailored to serve a compelling [governmental] interest.’”⁵⁴ Strict scrutiny reverses the burden of persuasion, requiring the government to defend its law.⁵⁵ Traditionally, “[s]ubstantive due process cases typically apply strict scrutiny in the case of a fundamental right and rational basis review in all other cases.”⁵⁶

In some cases, the Court applies neither of the traditional tests, but instead uses an intermediate standard of scrutiny,⁵⁷ sometimes called a “searching rational basis test.”⁵⁸ Under this standard, legislation must serve “important governmental objectives and must be substantially related to achievement of those objectives.”⁵⁹ Such cases represent neither a strict scrutiny standard, nor a mere rational basis test, but a more “searching constitutional inquiry”⁶⁰ tailored to the specific issue at

⁵⁰ *Cook v. Gates*, 528 F.3d 42, 55 (2008).

⁵¹ *See id.* at 55 (citing *Nordlinger v. Hahn*, 505 U.S. 1, 11–12 (1992); *Heller v. Doe*, 509 U.S. 312, 324 (1993)).

⁵² *See* GUNTHER & SULLIVAN, *supra* note 36, at 467.

⁵³ *Witt*, 527 F.3d at 817.

⁵⁴ *Glazner*, *supra* note 46, at 641 (citing *Watson v. Perry*, 918 F. Supp. 1403, 1416 (W.D. Wash. 1996); *City of Cleburne v. Cleburne Living Ctr.*, 473 U.S. 432, 440 (1985)).

⁵⁵ JEFFREY M. SHAMAN, *CONSTITUTIONAL INTERPRETATION: ILLUSION AND REALITY* 72 (2001).

⁵⁶ *Witt*, 527 F.3d at 817.

⁵⁷ Intermediate scrutiny rose to prominence during the 1970s in the context of equal rights challenges to gender discrimination. GUNTHER & SULLIVAN, *supra* note 36, at 683. For examples of intermediate scrutiny, see generally *Craig v. Boren*, 429 U.S. 190 (1976) and *Sell v. United States*, 539 U.S. 166 (2003).

⁵⁸ Robert I. Correales, *Don't Ask, Don't Tell: A Dying Policy on the Precipice*, 44 CAL. W. L. REV. 413, 441 (Spring 2008) (citing *United States v. Marcum*, 60 M.J. 198, 201 (C.A.A.F. 2004)).

⁵⁹ *Craig*, 429 U.S. at 197.

⁶⁰ *Marcum*, 60 M.J. at 205.

hand.⁶¹ These cases “shift away from the rigid two-tiered standard of review to a more flexible sliding-scale approach.”⁶²

D. History of DADT

1. Pre-Statutory Practice

Congress stated in the DADT policy that “[t]he prohibition against homosexual conduct is a longstanding element of military law that continues to be necessary.”⁶³ This language references the military practice, prior to DADT, of “total exclusion of homosexuals from the armed forces.”⁶⁴ Wholesale exclusion “was based upon notions that ‘[h]omosexuality is incompatible with military service’ and that the presence of homosexuals in the armed forces ‘seriously impairs the accomplishment of the military mission.’”⁶⁵ Exclusion was not statutory until World War I, when the military “pronounced that homosexuals were not only dangerous, but also ineffective fighters.”⁶⁶ Prohibition on homosexuals *per se* continued until 1993.⁶⁷

⁶¹ See generally *Sell*, 539 U.S. 166. In *Sell*, the *Cook* court found “instructive in the sense that it illustrates the Supreme Court’s application of an intermediate level of scrutiny.” *Cook v. Gates*, 528 F.3d 42, 60 (2008).

⁶² Anna Stolley Persky, *Don’t Ask, Don’t Tell, Don’t Work?*, ABA L.J. (Oct. 2008) (quoting Courtney Joslin, Law Professor, Univ. Cal. at Davis, referring to potential interpretations of *Lawrence*).

⁶³ 10 U.S.C. § 654(a)(13) (2006).

⁶⁴ Aaron A. Seamon, *The Flawed Compromise of 10 U.S.C. 654: An Assessment of the Military’s “Don’t Ask, Don’t Tell” Policy*, 24 DAYTON L. REV. 319, 324 (Winter 1999).

⁶⁵ *Id.* at 323–24 (citing 32 C.F.R. pt. 41, app. A, pt. 1, H (1992)).

⁶⁶ JILL NORGAN & SERENA NANDA, AMERICAN CULTURAL PLURALISM AND LAW 187 (2d ed. 1996).

⁶⁷ Seamon, *supra* note 64, at 323. Enforcement was not uniform, with some boards “recommending the retention of enlisted personnel who, but for their homosexuality, were exemplary soldiers. Headquarters, Department of the Army, concluding that this practice was at variance with the new policy, issued a release saying that the intent of the new policy was to permit retention only of nonhomosexual soldiers.” *Watkins v. U.S. Army*, 721 F.2d 687, 689 (9th Cir. 1983) (citing Message, 161400Z Jun 82, Headquarters, U.S. Dep’t of Army, paras. 4-5).

2. *The Statute: 10 U.S.C. § 654*⁶⁸

President Clinton signed the current DADT policy in 1993, pursuant to the National Defense Authorization Act for 1994,⁶⁹ after his efforts to abolish the prohibition on homosexuals in the military proved unpopular with Congress and the military.⁷⁰ The DADT policy does not explicitly require separation based upon homosexual status, but instead requires separation based upon findings that “the member has engaged in, attempted to engage in, or solicited another to engage in a homosexual act or acts.”⁷¹ The Department of Defense (DoD) interpreted this to mean that “[a] person’s sexual orientation is considered a personal and private matter and is not a bar to entry or continued service unless manifested by homosexual conduct[.]”⁷² Homosexual conduct, according to the statute, includes “engag[ing] in, attempt[ing] to engage in, or solicit[ing] another to engage in a homosexual act or acts,”⁷³ marrying or attempting to marry a person of the same sex,⁷⁴ or making a statement that one is “homosexual or bisexual, or words to that effect.”⁷⁵ A finding that any of these acts occurred requires separation unless it is further found that “the member has demonstrated that he or she is not a person who engages in, attempts to engage in, has a propensity to engage in, or intends to engage in homosexual acts.”⁷⁶ The burden of that showing rests with the member.⁷⁷

The DADT policy is based upon the congressional finding that “persons who demonstrate a propensity or intent to engage in homosexual acts would create an unacceptable risk to the high standards of morale, good order and discipline, and unit cohesion”⁷⁸ of military

⁶⁸ See app. A for the full text of 10 U.S.C. § 654 (2006).

⁶⁹ National Defense Authorization Act for Fiscal Year 1994, Pub. L. No. 103-160, § 571, 107 Stat. 1547 (1993).

⁷⁰ See Correales, *supra* note 58, at 416–18; Thomasson v. Perry, 80 F.3d 915, 921 (4th Cir. 1996) (providing a detailed account of “the legislative process that led to the enactment of § 654,” Cook v. Gates, 429 F.2d 385, 387 (2006)).

⁷¹ 10 U.S.C. § 654(b)(1).

⁷² U.S. DEP’T OF DEFENSE, INSTR. 1332.14, ENLISTED ADMINISTRATIVE SEPARATIONS encl. 3, pt. 8a(1) (28 Aug. 2008).

⁷³ 10 U.S.C. § 654(b)(1).

⁷⁴ *Id.* § 654(b)(3).

⁷⁵ *Id.* § 654(b)(2).

⁷⁶ *Id.*; see also Thomasson v. Perry, 80 F.3d 915, 920 (4th Cir. 1996).

⁷⁷ U.S. DEP’T OF ARMY, REG. 600-20, ARMY COMMAND POLICY para. 4-19d(5)(f) (Mar. 18, 2008) [hereinafter AR 600-20].

⁷⁸ 10 U.S.C. § 654(a)(15).

units. This broad finding and its statutory implementation do not “contemplate weighing the perceived deleterious effects of the presence of openly homosexual service members on morale, good order and discipline . . . against the individual merit or value of the service of any particular openly homosexual service member.”⁷⁹ Congress considers a person who engages in any act indicating homosexual tendencies a *per se* danger to military effectiveness,⁸⁰ no “matter how exemplary a service member’s performance has been.”⁸¹

3. Bowers—*The Old Regime*

The Supreme Court in *Bowers v. Hardwick* (*Bowers*)⁸² effectively foreclosed successful legal challenges to DADT.⁸³ There the Court, dealing with a Georgia sodomy law⁸⁴ criminalizing homosexual practices,⁸⁵ found no “fundamental right [for] homosexuals to engage in acts of consensual sodomy.”⁸⁶ The Court explicitly applied a rational basis test to the Georgia law and found that “the presumed belief of a majority of the electorate in Georgia that homosexual sodomy is immoral and unacceptable” was an adequate basis for the law.⁸⁷ Applied to DADT, this rationale provided a judicially solid foundation for holding

that the military ban on homosexual acts intruded upon no constitutionally protected right and was “rationally related” to legitimate military needs for “unit cohesion”

⁷⁹ *Cook v. Gates*, 429 F.2d 385, 390 (2006).

⁸⁰ 10 U.S.C. § 654(a)(15).

⁸¹ *Cook*, 429 F.2d at 391.

⁸² 478 U.S. 186 (1986), *overruled by* *Lawrence v. Texas*, 539 U.S. 558 (2003).

⁸³ Glazner, *supra* note 46, at 636.

⁸⁴ GA. CODE ANN. § 16-6-2 (2006) (“A person commits the offense of sodomy when he or she performs or submits to any sexual act involving the sex organs of one person and the mouth or anus of another.”). *Id.* para. (a)(1).

⁸⁵ *Bowers*, 478 U.S. at 188. Although the statute was drafted more broadly than acts specific to same sex couples, the Court narrowed its analysis to “Hardwick’s challenge to the Georgia statute as applied to consensual homosexual sodomy. We express no opinion on the constitutionality of the Georgia statute as applied to other acts of sodomy.” *Id.*

⁸⁶ *Id.* at 192.

⁸⁷ *Id.* at 196. See Anne B. Goldstein, *History, Homosexuality, and Political Values: Searching for the Hidden Determinants of Bowers v. Hardwick*, 97 YALE L.J. 1073 (May 1988) (discussing the role political bias among jurists may have played in *Bowers* and stating that, “competing political philosophies, classical conservatism and classical liberalism, respectively, underlie the Supreme Court majority and dissenting opinions”). Goldstein, *supra*, at 1091.

and discipline. Moreover, by equating the admission of homosexuality by individual service members—unless demonstrated otherwise—with “propensity” for illegal conduct, the “don’t ask, don’t tell” policy successfully avoided equal protection and first amendment challenge as well.⁸⁸

4. Lawrence—*The New Regime*

The Supreme Court in *Lawrence* overruled *Bowers*⁸⁹ and, with it, the foundation for prior judicial rulings concerning DADT.⁹⁰ The *Lawrence* Court considered the constitutionality of a Texas statute⁹¹ purporting to make it a crime for “two persons of the same sex to engage in certain intimate sexual conduct.”⁹² Relying upon the principles of personal freedom and individual liberty protected by the Fifth and Fourteenth Amendments, the Court found that Americans

are entitled to respect for their private lives. The State cannot demean their existence or control their destiny by making their private sexual conduct a crime. Their right to liberty under the Due Process Clause gives them the full right to engage in their conduct without intervention of the government. “It is a promise of the Constitution that there is a realm of personal liberty which the government may not enter.” The Texas statute furthers no legitimate state interest which can justify its intrusion into the personal and private life of the individual.⁹³

⁸⁸ DAVID F. BURRELLI & JODY FEDER, CONG. RESEARCH SERV., *HOMOSEXUALS AND THE U.S. MILITARY: CURRENT ISSUES*, RL 30113, at 14 (2008).

⁸⁹ *Lawrence v. Texas*, 539 U.S. 558, 578 (2003).

⁹⁰ *See United States v. Marcum*, 60 M.J. 198, 206–07 (C.A.A.F. 2004).

⁹¹ TEX. PENAL CODE ANN. § 21.06(a) (Vernon 2007). Unlike the Georgia statute upheld in *Bowers*, the Texas law specifically criminalized homosexual conduct, stating that “[a] person commits an offense if he engages in deviate sexual intercourse with another individual of the same sex.” *Id.*

⁹² *Lawrence*, 539 U.S. at 562.

⁹³ *Id.* at 578 (citations omitted) (quoting *Planned Parenthood of Se. Pa. v. Casey*, 505 U.S. 833, 847 (1992)).

The Court explained in detail its decision to overrule *Bowers*,⁹⁴ noting that “criticism of *Bowers* has been substantial and continuing, disapproving of its reasoning in all respects.”⁹⁵ In a powerful rejection of its prior rationale, the Court opined that *Bowers*’ “continuance as precedent demeans the lives of homosexual persons”⁹⁶ and that “*Bowers* was not correct when it was decided, and it is not correct today. It ought not to remain binding precedent. *Bowers v. Hardwick* should be and now is overruled.”⁹⁷ This dramatic holding cast new doubts upon the constitutionality of Congress’s broad prohibition of homosexuality in the military.⁹⁸ In the wake of the Court’s discussion of “gay and lesbian sexual conduct in grand terms of liberty,”⁹⁹ the “bulwark of *Bowers* has crumbled, arming opponents of [Uniform Code of Military Justice] Article 125,¹⁰⁰ and ‘don’t ask, don’t tell,’ with an argument that current military policies abridge the due process right to privacy of homosexual service members.”¹⁰¹

Efforts to interpret the Supreme Court’s language in *Lawrence*¹⁰² dominate the present debate concerning the legal status of DADT.¹⁰³ There is much confusion on this point¹⁰⁴ because, despite its grand language, *Lawrence* did not specify a constitutional standard of review.¹⁰⁵ The “precise standard of judicial review, in the wake of *Lawrence* . . . has yet to be firmly established.”¹⁰⁶

⁹⁴ *Id.*

⁹⁵ *Id.* at 575 (noting that even the “courts of five different States have declined to follow [*Bowers*] in interpreting provisions in their own state constitutions parallel to the Due Process Clause of the Fourteenth Amendment.”). *Id.*

⁹⁶ *Id.*

⁹⁷ *Id.* at 578.

⁹⁸ Glazner, *supra* note 46, at 644–48.

⁹⁹ *Id.*

¹⁰⁰ The military’s criminal statute prohibiting sodomy, located at MANUAL FOR COURTS-MARTIAL, UNITED STATES pt. IV, para. 51 (2008) [hereinafter MCM].

¹⁰¹ BURRELLI & FEDER, *supra* note 88, at 14.

¹⁰² See Cook v. Rumsfeld, 429 F. Supp. 2d 385, 395 (D. Mass. 2006); United States v. Marcum, 60 M.J. 198, 204 (C.A.A.F. 2004) (providing examples of linguistic hairsplitting of *Lawrence*); Brief of Appellant-Petitioner at 49-51, Witt v. Dep’t of the Air Force, No. 06-35644 (9th Cir. Oct. 16, 2006).

¹⁰³ See, e.g., Witt v. Dep’t of the Air Force, 527 F.3d 806 (2008); Cook v. Gates, 528 F.3d 42 (2008); Marcum, 60 M.J. at 206–07; Glazner, *supra* note 46, at 635.

¹⁰⁴ See generally Persky, *supra* note 62.

¹⁰⁵ See Witt, 527 F.3d at 814; Cook, 528 F.3d at 49.

¹⁰⁶ BURRELLI & FEDER, *supra* note 88, at 14.

III. Discussion

A. Split in the Circuits

In two recent cases, the Ninth Circuit Court of Appeals and the First Circuit Court of Appeals confronted the question of the post-*Lawrence* standard of review,¹⁰⁷ something the federal appellate courts had yet to address.¹⁰⁸ Both cases involved challenges to DADT by servicemembers, and both cases were dismissed¹⁰⁹ for failure to state a claim.¹¹⁰ Though both courts applied intermediate standards of review,¹¹¹ they differed in their interpretations of *Lawrence* and its impact on DADT.¹¹² Ultimately, the Ninth Circuit remanded¹¹³ the matter back to the district court, while the First Circuit issued a ruling in the case.¹¹⁴ This article examines each in turn, starting with *Witt*.

1. *The Ninth Circuit's Due Process Analysis*

The Ninth Circuit noted that “[b]ecause *Lawrence* is, perhaps intentionally so, silent as to the level of scrutiny that it applied, both parties draw upon language from *Lawrence* that supports their views.”¹¹⁵ Observing that in *United States v. Marcum*¹¹⁶ the U.S. Court of Appeals for the Armed Forces’ (CAAF)¹¹⁷ became frustrated with a semantic

¹⁰⁷ See generally *Witt*, 527 F.3d 806; *Cook*, 528 F.3d at 55 n.1; Persky, *supra* note 62.

¹⁰⁸ *Witt*, 527 F.3d at 815 (“[T]he Eleventh Circuit upheld a law that forbade homosexuals from adopting children, explicitly holding that *Lawrence* did not apply strict scrutiny. Otherwise, our sister circuits are silent.”).

¹⁰⁹ *Id.* at 809; *Cook*, 528 F.3d at 45 n.1.

¹¹⁰ FED. R. CIV. P. 12(b)(6) allows a court, upon pre-trial motion, to dismiss a case for “failure to state a claim upon which relief can be granted.”

¹¹¹ *Witt*, 527 F.3d at 819; *Cook*, 528 F.3d at 56.

¹¹² *Cook* 528 F.3d at 45 n.1 (acknowledging the decision in *Witt* and stating that, “we resolve differently the as applied substantive due process claim brought in this case.”); BURRELLI & FEDER, *supra* note 88, at 20–22.

¹¹³ *Witt*, 527 F.3d at 822.

¹¹⁴ *Cook*, 528 F.3d at 65.

¹¹⁵ *Witt*, 527 F.3d at 814 (2008) (emphasis added).

¹¹⁶ 60 M.J. 198 (C.A.A.F. 2004).

¹¹⁷ The CAAF is an appellate court comprised of five civilian judges with jurisdiction over personnel subject to the Uniform Code of Military Justice (UCMJ). Its decisions are generally appealable to the U.S. Supreme Court. See U.S. Court of Appeals for the Armed Forces, <http://www.armfor.uscourts.gov> (last visited Feb. 15, 2009).

approach to interpreting *Lawrence*,¹¹⁸ the Ninth Circuit elected to analyze *Lawrence* “by considering what the Court actually *did*, rather than by dissecting isolated pieces of text.”¹¹⁹ In doing so, the court observed that the Supreme Court in *Lawrence* overturned *Bowers*, the critical case rejecting the idea of a protected interest in “adult persons in deciding how to conduct their private lives in matters pertaining to sex,”¹²⁰ and in particular homosexual intimacy,¹²¹ not because it lacked a rational basis, but “because of the ‘Court’s own failure to appreciate the extent of the liberty at stake.’”¹²² The *Lawrence* Court’s consideration of the liberty interest affected by the subject legislation was “inconsistent with rational basis review,”¹²³ in the opinion of the Ninth Circuit, because only “the basis for the law”¹²⁴ typically merits consideration in a rational basis analysis.¹²⁵ The Ninth Circuit also took note of the public policy rationale provided in *Lawrence*, stating that “the Court overturned *Bowers* because ‘[i]ts continuance as precedent demeans the lives of homosexual persons.’”¹²⁶

To address the specific question of homosexual conduct in the military, the Ninth Circuit looked to the military court’s application of *Lawrence* in *Marcum*, which involved homosexual sodomy.¹²⁷ It cited the CAAF analysis in *Marcum* for the proposition that, even in the military, the implications of *Lawrence* must be considered in the context of each specific case, not through a broad challenge to the DADT policy.¹²⁸ The Ninth Circuit found especially instructive that the *Marcum* court undertook a detailed, fact-specific analysis based upon its

¹¹⁸ *Witt*, 527 F.3d at 816 (“[A]s the Court of Appeals for the Armed Forces stated in *Marcum*, ‘[a]lthough particular sentences within the Supreme Court’s opinion may be culled in support of the Government’s argument, other sentences may be extracted to support Appellant’s argument.’”) (quoting *United States v. Marcum*, 60 M.J. 198, 204 (C.A.A.F. 2004) (citation omitted)).

¹¹⁹ *Id.*

¹²⁰ *Lawrence v. Texas*, 539 U.S. 558, 572 (2003).

¹²¹ *Bowers v. Hardwick*, 478 U.S. 186, 191 (1986), *overruled by Lawrence v. Texas*, 539 U.S. 558 (2003) (announcing the refusal of the Court to create “a fundamental right to engage in homosexual sodomy.”).

¹²² *Witt*, 527 F.3d at 817 (quoting *Lawrence*, 539 U.S. at 567).

¹²³ *Id.*

¹²⁴ *Id.*

¹²⁵ *Id.*; see also Part II.C, *infra*.

¹²⁶ *Witt*, 527 F.3d at 817 (quoting *Lawrence*, 539 U.S. at 575).

¹²⁷ *Id.* at 816.

¹²⁸ *Id.* (quoting *United States v. Marcum*, 60 M.J. 198, 206 (C.A.A.F. 2004)).

interpretation of *Lawrence*.¹²⁹ In view of the fact-specific analysis in *Marcum*, the Ninth Circuit concluded that CAAF applied more than a rational basis review to the sodomy rule as it applied to homosexuality. The court stated that by “considering whether the policy applied properly to a particular litigant, rather than whether there was a permissible application of the statute, the court necessarily required more than hypothetical justification for the policy—all that is required for rational basis review.”¹³⁰

Having found that both CAAF and the *Lawrence* Court “applied something more than traditional rational basis review”¹³¹ to laws addressing homosexual conduct, the Ninth Circuit rejected the other traditional standard, strict scrutiny. The court noted that the language normally found in strict scrutiny cases, such as “narrow tailoring or a compelling state interest,”¹³² was noticeably absent from the *Lawrence* opinion.¹³³ The Ninth Circuit declined to read the highest constitutional standard into a decision that did not explicitly require it.¹³⁴ Despite this apparent deference, Justice Canby’s dissenting assertion that “the right to engage in homosexual relationships and related private sexual conduct is a personal right of a high constitutional order, and that the ‘Don’t Ask, Don’t Tell’ statute so penalizes that relationship and conduct that it must be subjected to strict scrutiny,”¹³⁵ and the majority’s observation that “DADT most likely would not” survive strict scrutiny,¹³⁶ imply that the Ninth Circuit takes a dim view of the policy.

¹²⁹ *Marcum* dealt with a challenge to the UCMJ provision criminalizing sodomy. The *Witt* court took note of the following test:

First, was the conduct that the accused was found guilty of committing of a nature to bring it within the liberty interest identified by the Supreme Court? Second, did the conduct encompass any behavior or factors identified by the Supreme Court as outside the analysis in *Lawrence*? Third, are there additional factors relevant solely in the military environment that affect the nature and reach of the *Lawrence* liberty interest?

Id. (quoting *Marcum*, 60 M.J. at 206-07).

¹³⁰ *Id.*

¹³¹ *Id.* at 817.

¹³² *Id.*

¹³³ *Id.*

¹³⁴ *Id.*

¹³⁵ *Id.* at 823.

¹³⁶ *Id.* at 817.

Stopping short of radical measures, the Ninth Circuit instead turned to the Supreme Court's careful balancing of state interests against individual liberties in *Sell v. United States* (*Sell*)¹³⁷ for guidance in formulating an intermediate standard of review.¹³⁸ Although *Sell* dealt with "forcibly administering medication, the scrutiny employed by the Court . . . is instructive,"¹³⁹ as it "resembles and expands upon the analysis performed in *Lawrence*."¹⁴⁰ The Ninth Circuit observed that the Court in *Sell*

recognized a "significant" liberty interest—the interest "in avoiding the unwanted administration of antipsychotic drugs"—and balanced that liberty interest against the "legitimate" and "important" state interest "in providing appropriate medical treatment to reduce the danger that an inmate suffering from a serious mental disorder represents to himself or others."¹⁴¹

Noting the consistency of this approach with Supreme Court precedent along intermediate scrutiny lines,¹⁴² the Ninth Circuit described how, in order "[t]o balance those two interests, the [*Sell*] Court required the state to justify its intrusion into an individual's recognized liberty interest against forcible medication—just as *Lawrence* determined that the state had failed to 'justify its intrusion into the personal and private life of the individual.'"¹⁴³

In *Sell* the Supreme Court noted that "[a] compelled surgical intrusion into an individual's body . . . implicates expectations of privacy and security' of great magnitude."¹⁴⁴ The Court stated that "the Constitution permits the Government involuntarily to administer antipsychotic drugs to a mentally ill defendant facing serious criminal charges in order to render that defendant competent to stand trial, but only if"¹⁴⁵ four criteria are satisfied. First, the court must find that

¹³⁷ 539 U.S. 166 (2003).

¹³⁸ *Witt*, 527 F.3d at 818.

¹³⁹ *Id.*

¹⁴⁰ *Id.*

¹⁴¹ *Id.* (quoting *Sell*, 539 U.S. at 178).

¹⁴² *Id.* at 818 n.7 (citing *Craig v. Boren*, 429 U.S. 190, 197 (1976)).

¹⁴³ *Id.* at 818 (discussing *Sell*, 539 U.S. 166) (quoting *Lawrence v. Texas*, 539 U.S. 558, 578 (2003)).

¹⁴⁴ *Sell*, 539 U.S. at 176 (quoting *Winston v. Lee*, 470 U.S. 753, 759 (1985)).

¹⁴⁵ *Id.* at 179.

“important governmental interests are at stake.”¹⁴⁶ Second, if such an interest is identified, the court must find “that involuntary medication will *significantly further* those concomitant state interests.”¹⁴⁷ Third, the court must find that the use of medication is “*necessary* to further those interests.”¹⁴⁸ Finally, “the court must conclude that administration of the drugs is *medically appropriate*.”¹⁴⁹ Following its restatement of the *Sell* criteria, the Ninth Circuit performed an analysis particularized to the facts of the *Witt* case.¹⁵⁰

The Ninth Circuit adapted the *Sell* factors to weigh the rights of the individual against the military’s concerns as addressed in DADT.¹⁵¹ Dismissing the fourth factor as “specific to the medical context of *Sell*,”¹⁵² the court said that “the first three factors apply equally”¹⁵³ to a challenge to DADT. The court extracted the underlying principles from their original, medical context and stated them more broadly, holding

that when the government attempts to intrude upon the personal and private lives of homosexuals, in a manner that implicates the rights identified in *Lawrence*, the government must advance an important governmental interest, the intrusion must significantly further that interest, and the intrusion must be necessary to further that interest. In other words, for the third factor, a less intrusive means must be unlikely to achieve substantially the government’s interest.¹⁵⁴

The court further held that “this heightened scrutiny analysis is as-applied rather than facial.”¹⁵⁵ This holding is based upon *Sell*’s requirement that courts “consider the facts of the individual case in evaluating the Government’s interest”¹⁵⁶ as well as the principle that as-applied analysis “is the preferred course of adjudication since it enables

¹⁴⁶ *Id.* at 180 (emphasis added).

¹⁴⁷ *Id.* at 181 (emphasis added).

¹⁴⁸ *Id.* (emphasis added).

¹⁴⁹ *Id.* (emphasis added).

¹⁵⁰ *Id.* at 176–81.

¹⁵¹ *Witt v. Dep’t of the Air Force*, 527 F.3d 806, 819 (2008).

¹⁵² *Id.* (emphasis added).

¹⁵³ *Id.*

¹⁵⁴ *Id.* (emphasis added).

¹⁵⁵ *Id.*

¹⁵⁶ *Id.* (quoting *Sell v. United States*, 539 U.S. 166, 180 (2003)).

courts to avoid making unnecessarily broad constitutional judgments.”¹⁵⁷ The court claimed to take “direction from the Supreme Court”¹⁵⁸ in reaching this conclusion. It did so by reasoning itself “bound by the theory or reasoning underlying a Supreme Court case, not just by its holding.”¹⁵⁹ The Ninth Circuit cited itself for this versatile proposition.¹⁶⁰

Applying the *Sell* factors to the facts in *Witt*, the Ninth Circuit held that “the government advances an important governmental interest . . . the management of the military.”¹⁶¹ This judicial finding satisfied the first prong of the court’s application of “heightened scrutiny to DADT in light of current Supreme Court precedents.”¹⁶² However, the court ended its analysis with the first prong because the record lacked evidence particular to Major Witt’s case. The court could not answer “whether the application of DADT specifically to Major Witt significantly furthers the government’s interest and whether less intrusive means would achieve substantially the government’s interest.”¹⁶³ Based upon this lack of particularized evidence,¹⁶⁴ the Ninth Circuit remanded the case to “the district court to develop the record.”¹⁶⁵ In a footnote to its instruction, the court noted that the Air Force would not likely produce such evidence, given that “Major Witt was a model officer whose sexual activities hundreds of miles away from base did not affect her unit until the military initiated discharge proceedings under DADT and, even then, it was her suspension pursuant to DADT, not her homosexuality, that damaged unit cohesion.”¹⁶⁶

¹⁵⁷ *Id.* (quoting *City of Cleburne v. Cleburne Living Ctr., Inc.*, 473 U.S. 432, 447 (1985)).

¹⁵⁸ *Id.*

¹⁵⁹ *Id.* (quoting *Miller v. Gammie*, 335 F.3d 889, 900 (9th Cir. 2003)).

¹⁶⁰ *Id.* at 818.

¹⁶¹ *Id.* at 821; *see also* Brief of Appellee-Respondent at 13–14, *Witt v. Dep’t of the Air Force*, No. 06-35644 (9th Cir. Jan. 3, 2007).

¹⁶² *Witt*, 527 F.3d at 821.

¹⁶³ *Id.*

¹⁶⁴ *Id.*

¹⁶⁵ *Id.*

¹⁶⁶ *Id.* at 821 n.11. The *Witt* court was a three-member panel reviewing the district court’s decision to dismiss Major Witt’s complaint under Federal Rule 12(b)(6). By holding in this way, the panel appears to have predetermined the outcome of any further proceedings at the district level. As of this writing, the Air Force had undertaken no further action on this case. *See* Telephone Interview with James E. Lobsenz, Shareholder, Carney Badley Spellman, P.S., and Adjunct Professor, Seattle University School of Law, in Seattle, Wash. (Dec. 20, 2008) [hereinafter Lobsenz Telephone Interview].

2. *The Ninth Circuit's Equal Protection Analysis*

The Ninth Circuit did not confront the implications of *Lawrence* for its equal protection precedent with respect to DADT,¹⁶⁷ nor did it address the equal protection arguments raised in Major Witt's appellate brief.¹⁶⁸ Instead, it disposed of Major Witt's equal protection argument summarily,¹⁶⁹ relying entirely on its 1997 holding in *Phillips v. Perry* (*Phillips*)¹⁷⁰ for the proposition that "DADT does not violate equal protection under rational basis review, and that holding was not disturbed by *Lawrence*."¹⁷¹

A closer reading of *Phillips* reveals some irony in the court's logic. As explained in the dissenting opinion by Judge Canby,¹⁷² the *Phillips* court relied entirely upon its 1990 opinion in *High Tech Gays v. Defense Industrial Security Clearance Office* (*High Tech Gays*)¹⁷³ for the proposition that "homosexuals do not constitute a suspect or quasi-suspect class entitled to greater than rational basis scrutiny under the equal protection component of the Due Process Clause of the Fifth Amendment."¹⁷⁴ *High Tech Gays*, in turn, relied entirely upon the Supreme Court's statement in *Bowers* "that homosexual activity is not a fundamental right protected by substantive due process and that the proper standard of review under the Fifth Amendment is rational basis review."¹⁷⁵ The Ninth Circuit heightened the irony of its apparently inadvertent reliance on *Bowers* when it reasoned that *Lawrence* did not disturb its holding in *Phillips* precisely because the Supreme Court was

¹⁶⁷ The court merely recited Major Witt's argument in summary, stating "[s]he argues that DADT violates equal protection because the Air Force has a mandatory rule discharging those who engage in homosexual activities but not those 'whose presence may also cause discomfort among other service members,' such as child molesters." *Witt*, 527 F.3d at 821.

¹⁶⁸ See generally Brief of Appellant-Petitioner, *Witt v. Dep't of the Air Force*, No. 06-35644 (9th Cir. Oct. 16, 2006).

¹⁶⁹ In its twelve-page opinion, the majority devotes a single paragraph, 116 words, to Major Witt's equal protection claim.

¹⁷⁰ 106 F.3d 1420 (1997). *Phillips* involved a military member who, like Major Witt, claimed "that his sexual encounters never involved other military members or occurred on board ship or on a military installation; that the acts were consensual; that he had experienced no problems at work because of his homosexuality." *Id.* at 1422.

¹⁷¹ *Witt*, 527 F.3d at 821 (internal citations omitted).

¹⁷² *Id.* at 822–27 (2008).

¹⁷³ 895 F.2d 563 (1990).

¹⁷⁴ *Phillips*, 106 F.3d at 1425 (quoting *High Tech Gays*, 895 F.2d at 574).

¹⁷⁵ *High Tech Gays*, 895 F.2d at 571 (citing *Bowers v. Hardwick*, 478 U.S. 186 (1986)).

focused on “whether *Bowers* itself ha[d] continuing validity.”¹⁷⁶ As Judge Canby explained, “[b]ecause Lawrence unequivocally overruled *Bowers*, it ‘undercut the theory [and] reasoning underlying’ *High Tech Gays* and *Philips* ‘in such a way that the cases are clearly irreconcilable.’”¹⁷⁷

The circuit court’s equal protection analysis closely resembled the almost equally cursory¹⁷⁸ treatment by the district court.¹⁷⁹ The district court cited *Philips* as an example of the law before *Lawrence*¹⁸⁰ and did not explicitly rely upon it as authority for its dismissal of the equal protection complaint.¹⁸¹ It cited instead to another pre-*Lawrence* decision, *Holmes v. California Army Nat’l Guard (Holmes)*,¹⁸² which closely resembled the reasoning of *Philips* in the Ninth Circuit.¹⁸³ In *Holmes* the Ninth Circuit said it was “guided in [the equal protection] inquiry by our recent decision in *Philips v. Perry*, in which we upheld the acts prong of § 654(b)(1) against an equal protection challenge.”¹⁸⁴ The court in *Holmes* then recited substantially the same language as *Philips*, resulting in the same indirect reliance on discredited precedent.¹⁸⁵ The *Holmes* court’s substantive due process analysis further demonstrated its inappropriateness in a post-*Lawrence* discussion of DADT by stating in its entirety,

We have previously rejected claims similar to Watson’s substantive due process claim. See *Schowengerdt v. United States*, 944 F.2d 483, 490 (9th Cir. 1991) (stating that substantive due process claim with respect to the old policy was foreclosed by *Bowers v. Hardwick*, 478 U.S.

¹⁷⁶ *Witt*, 527 F.3d at 821 (quoting *Lawrence v. Texas*, 539 U.S. 558, 574–75 (2003)). Major Witt asserts in her brief to the Ninth Circuit that *Phillips* was wrongly decided. Brief of Appellant-Petitioner at 49, *Witt v. Dep’t of the Air Force* (9th Cir. Oct. 16, 2006) (No. 06-35644).

¹⁷⁷ *Witt*, 527 F.3d at 824 (Canby, J., dissenting) (quoting *Miller v. Gammie*, 335 F.3d 889, 900 (9th Cir. 2003)) (emphasis added).

¹⁷⁸ One hundred forty-five words, divided into two paragraphs.

¹⁷⁹ *Witt v. Dep’t of the Air Force*, 444 F. Supp. 2d 1138, 1145 (W.D. Wash. 2006).

¹⁸⁰ *Id.* at 1144.

¹⁸¹ *See id.* at 1145.

¹⁸² 124 F.3d 1126 (1997).

¹⁸³ *Philips* was filed on 18 April 1997. *Holmes* was filed 5 September 1997.

¹⁸⁴ *Holmes*, 124 F.3d at 1132 (internal citation omitted).

¹⁸⁵ *Id.*

186, 92 L. Ed. 2d 140, 106 S. Ct. 2841 (1986), Beller, and High Tech Gays).¹⁸⁶

Relying on pre-*Lawrence* precedent, which was based entirely on the discredited opinion in *Bowers*, both the district and circuit courts in *Witt* failed to address the *Lawrence* Court's impact on the equal protection analysis.

Major Witt raised a novel equal protection argument to illustrate the inappropriateness of DADT as it is currently applied. She observed in her brief that while separation for homosexual conduct is mandatory, the military "does not have a mandatory rule discharging other people whose presence may also cause discomfort among other service members: namely, persons who commit a variety of crimes society condemns as loathsome."¹⁸⁷ She cited as an example an Air Force regulation which authorizes, but does not require, separation of servicemembers who molest children.¹⁸⁸ The Ninth Circuit majority did not compare or address the merits of this challenge¹⁸⁹ in regard to the statutory rationale of DADT but instead merely disregarded it under *Phillips*.¹⁹⁰

Judge Canby, in his dissent, offered a more nuanced equal protection analysis. He offered that strict scrutiny should be applied to DADT on two grounds: classification of homosexuals as a suspect class under equal protection principles and the fundamental right to enjoy private intimacy under due process.¹⁹¹ In support of the qualification of homosexual persons as a suspect class, Judge Canby observed

that homosexuals have "experienced a history of purposeful unequal treatment [and] been subjected to unique disabilities on the basis of stereotyped characteristics not truly indicative of their abilities." They also "exhibit obvious, immutable, or distinguishing

¹⁸⁶ *Id.* at 1136.

¹⁸⁷ Brief of Appellee-Respondent at 50, *Witt v. Dep't of the Air Force*, No. 06-35644 (9th Cir. Jan. 3, 2007).

¹⁸⁸ *Id.*

¹⁸⁹ Major Witt's attorney described his decision not to raise a broad equal protection argument as a tactical one, explaining that "if I cannot win this on substantive due process in front of a panel, I certainly will not win on equal protection." Lobsenz Telephone Interview, *supra* note 166.

¹⁹⁰ *Witt v. Dep't of the Air Force*, 527 F.3d 806, 821 (2008).

¹⁹¹ *Id.* at 824 (Canby, J., dissenting).

characteristics that define them as a discrete group; and they are [] a minority.” In short, they are a group deserving of protection against the prejudices and power of an often-antagonistic majority.¹⁹²

Judge Canby argued that the right to engage in homosexual relationships falls squarely under an equal protection analysis, noting the *Lawrence* Court’s concession “that a decision recognizing a liberty interest in certain conduct advanced the cause of equality as well as due process.”¹⁹³ He observed that the Supreme Court sought other grounds specifically because it “would not sufficiently establish the right to intimate homosexual relations if only equal protection were invoked, because a state might frustrate the right by denying heterosexuals as well as homosexuals the right to non-marital sexual relations.”¹⁹⁴

Judge Canby argued that “[t]he reason for including an equal protection analysis is that there is a very clear element of discrimination in the whole ‘Don’t Ask, Don’t Tell’ apparatus.”¹⁹⁵ The equal protection analysis goes directly to the question, “what compelling interest of the Air Force is narrowly served by discharging homosexuals but not others who engage in sexual relations privately off duty, off base, and with persons unconnected to the military?”¹⁹⁶ While Judge Canby’s arguments did not convince the Ninth Circuit, his analysis demonstrates how DADT would fare under strict scrutiny.¹⁹⁷

3. *The First Circuit’s Due Process Analysis*

This article now addresses the First Circuit’s decision in *Cook*. The First Circuit, like the Ninth, determined that “interpreting *Lawrence* is the critical first step in evaluating the plaintiffs’ substantive due process claim.”¹⁹⁸ The First Circuit also agreed with the Ninth that *Lawrence*

¹⁹² *Id.* (quoting *Mass. Bd. of Ret. v. Murgia*, 427 U.S. 307, 313 (1976) and *Lyng v. Castillo*, 477 U.S. 635, 638 (1986)) (citations omitted).

¹⁹³ *Id.* at 825 (citing *Lawrence v. Texas*, 539 U.S. 558, 575 (2003)).

¹⁹⁴ *Id.* (citing *Lawrence*, 539 U.S. at 575).

¹⁹⁵ *Id.* at 826.

¹⁹⁶ *Id.*

¹⁹⁷ *Id.* at 827 (“[T]he Air Force must demonstrate that the ‘Don’t Ask, Don’t Tell’ statute meets the requirements of strict scrutiny—that it is necessary to serve a compelling governmental interest and that it sweeps no more broadly than necessary.”).

¹⁹⁸ *Cook v. Gates*, 528 F.3d 42, 49 (2008) (emphasis added).

requires “a standard of review that lies between strict scrutiny and rational basis.”¹⁹⁹ From there, however, the opinions diverge. The First Circuit noted that, “[i]n *Witt*, the 9th Circuit resolved an as-applied, post-*Lawrence* substantive due process challenge to [DADT] differently than we do here.”²⁰⁰

The circuit court began its analysis with a review of the district court opinion.²⁰¹ The district court determined that the rational basis standard of review continued to apply to legislation affecting private sexual conduct,²⁰² though it confessed that “the matter is not free from doubt because of the ambiguity of the *Lawrence* opinion.”²⁰³ Prior to engaging in a linguistic analysis of the terms used in the *Lawrence* decision, the district court explained that

the *Lawrence* majority did not expressly—that is, in so many words—recognize a fundamental liberty interest in “consensual intimacy and relationships between adults of the same sex.” One might stop right there. After all, for a proposition to be considered a holding, one might reasonably expect it to have been stated. This is particularly so when the proposition would state a new—that is, not previously announced—principle of constitutional law.²⁰⁴

The First Circuit did not agree, stating that “at least four reasons [support] reading *Lawrence* as recognizing a protected liberty interest. First, *Lawrence* relies on the following due process cases for doctrinal support: *Griswold*, *Eisenstadt*, *Roe*, *Carey*, and *Casey*.”²⁰⁵ Each of these, the court explained, “resulted in the Supreme Court recognizing a due process right to make personal decisions related to sexual conduct that mandated the application of heightened judicial scrutiny.”²⁰⁶

Second, the court relied upon the language of the *Lawrence* opinion, reciting the Court’s concern with matters such as “freedom of thought,

¹⁹⁹ *Id.* at 56.

²⁰⁰ *Id.* at 60 n.10 (citing *Witt*, 527 F.3d 806) (emphasis added).

²⁰¹ *Id.* at 47.

²⁰² *Cook v. Rumsfeld*, 429 F. Supp. 2d 385, 396 (D. Mass. 2006).

²⁰³ *Id.* at 395 (emphasis added).

²⁰⁴ *Id.* at 394 (emphasis added).

²⁰⁵ *Cook*, 528 F.3d at 52 (citations omitted) (emphasis added).

²⁰⁶ *Id.*

belief, and expression”²⁰⁷ and the statement that “[i]t is a promise of the Constitution that there is a realm of personal liberty which the government may not enter.”²⁰⁸ The court found *Lawrence*’s use of these broad terms of liberty “strongly suggest[ive] that *Lawrence* identified a protected liberty interest.”²⁰⁹

Third, the circuit court pointed out *Lawrence*’s reliance on the *Bowers* dissent as the controlling law.²¹⁰ The First Circuit specifically recalled Justice Stevens’s argument, also quoted in *Lawrence*,²¹¹ that “individual decisions by married persons, concerning the intimacies of their physical relationship, even when not intended to produce offspring, are a form of liberty protected by the Due Process Clause Moreover, this protection extends to intimate choices by unmarried as well as married persons.”²¹² Justice Stevens’s description of this liberty as fundamental²¹³ persuaded the First Circuit that it could not “read *Lawrence* as declining to recognize a protected liberty interest without ignoring the Court’s statement that Justice Stevens’ *Bowers* dissent was controlling.”²¹⁴

Finally, the First Circuit observed that the *Lawrence* Court overturned the convictions of those prosecuted under the Texas law,²¹⁵ noting that “prohibiting immoral conduct was the only state interest that Texas offered to justify the statute.”²¹⁶ Since the Court had acknowledged morality as a rational basis in the past,²¹⁷ the *Lawrence* case must have dealt with a liberty interest too important to give way before a mere rational basis.²¹⁸

For these reasons the First Circuit overruled the district court’s interpretation of *Lawrence* as applying a rational basis analysis to laws governing private, consensual sexual conduct,²¹⁹ holding that “*Lawrence*

²⁰⁷ *Id.* (quoting *Lawrence v. Texas*, 539 U.S. 558, 563 (2003)).

²⁰⁸ *Id.* (quoting *Lawrence*, 539 U.S. at 578).

²⁰⁹ *Id.* (emphasis added).

²¹⁰ *Id.* (citing *Lawrence*, 539 U.S. at 578).

²¹¹ *Lawrence*, 539 U.S. at 578.

²¹² *Cook*, 528 F.3d at 52 (quoting *Lawrence*, 539 U.S. at 578).

²¹³ *Bowers v. Hardwick*, 478 U.S. 186, 216 (1986) (Stevens, J., dissenting).

²¹⁴ *Cook*, 528 F.3d at 52 (emphasis added).

²¹⁵ *Id.* at 52.

²¹⁶ *Id.*

²¹⁷ *Id.* (citing *Barnes v. Glen Theatre, Inc.*, 501 U.S. 560, 569, (1991)).

²¹⁸ *Id.* at 53.

²¹⁹ *Id.*

did indeed recognize a protected liberty interest for adults to engage in private, consensual sexual intimacy and applied a balancing of constitutional interests that defies either the strict scrutiny or rational basis label.”²²⁰

The *Cook* court nods to *Sell* only to distinguish the review in *Lawrence* from strict scrutiny, stating that

in *Sell v. United States*, the Court recognized a “constitutionally protected liberty interest [for a criminal defendant] in avoiding the unwanted administration of antipsychotic drugs” and then applied a standard of review less demanding than strict scrutiny by asking whether administering the drugs was “necessary significantly to further important governmental trial-related interests.”²²¹

Unlike *Witt*, the First Circuit does not rely upon *Sell* for additional guidance in applying intermediate scrutiny, explaining that “[a]lthough we find *Sell* instructive in the sense that it illustrates the Supreme Court’s application of an intermediate level of scrutiny, we do not find *Sell* especially helpful in analyzing this statute regulating military affairs.”²²²

The First Circuit distinguished *Cook* from *Witt* by characterizing its case as a facial challenge to DADT.²²³ According to the court, the plaintiffs’ in *Cook* claimed the military policy unconstitutionally punishes acts protected by the liberty interest identified in *Lawrence*, namely “consensual sexual intimacy in the confines of one’s home and one’s own private life.”²²⁴ The court distinguished this argument from the matter before the Ninth Circuit in *Witt*, quoting the district court’s conclusion that

none of the plaintiffs claim that the policy, if valid in general, was misapplied in his or her particular case to result in separation when a proper application of the policy would have allowed him or her to remain in

²²⁰ *Id.* at 52 (emphasis added).

²²¹ *Id.* at 55 (citing *Sell v. United States*, 539 U.S. 166, 179 (2003)) (emphasis added).

²²² *Id.* at 60 (emphasis added).

²²³ *Id.* at 56.

²²⁴ *Id.* (citing *Lawrence v. Texas*, 539 U.S. 558, 567 (2003)).

service. Rather, their objections . . . are that the policy was applied, not how it was applied.²²⁵

The First Circuit observed that DADT “provides for the separation of a service person who engages in a public homosexual act or who coerces another person to engage in a homosexual act. Both of these forms of conduct are expressly excluded from the liberty interest recognized by *Lawrence*.”²²⁶ The First Circuit recited settled law to show why such a broad facial challenge to DADT must fail, stating that “[t]he fact that [an act] might operate unconstitutionally under some conceivable set of circumstances is insufficient to render it wholly invalid” in all circumstances.²²⁷

Since this First Circuit analysis treated the due process claim as “a facial challenge to the statute”²²⁸ and not as a challenge to its specific application to the plaintiffs’ facts, this aspect of the First Circuit’s opinion would not necessarily contradict the “as-applied” analysis in *Witt*.²²⁹ Jurists could simply read *Witt*’s facts as an example of an unconstitutional application of a potentially lawful policy.²³⁰ The Ninth Circuit focused narrowly on the particulars of its case.²³¹ It performed a fact-specific balancing test to the application of DADT, not to its destruction.²³² Neither case indicates that DADT itself fails a facial due process challenge.²³³

Disposing of the facial challenge, the First Circuit attempted an as-applied analysis of the statute’s application to its particular plaintiffs.²³⁴

²²⁵ *Id.* at 48 (citing the district court opinion at *Cook v. Rumsfeld*, 429 F. Supp. 2d 385 (D. Mass. 2006)).

²²⁶ *Id.* at 56 (citing *Lawrence*, 539 U.S. at 578) (emphasis added).

²²⁷ *Id.* (quoting *United States v. Salerno*, 481 U.S. 739, 745, (1987)).

²²⁸ *Id.* at 48 (citing the district court opinion at *Cook v. Rumsfeld*, 429 F. Supp. 2d 385 (D. Mass. 2006)).

²²⁹ *Witt v. Dep’t of the Air Force*, 527 F.3d 806, 819 (2008).

²³⁰ *Id.* (holding that the *Sell* factors are to be applied to each particular application of DADT).

²³¹ *Id.* at 810–13 (undertaking a detailed analysis of Major Witt’s procedural posture, the eligibility of the facts alleged to proceed as pleaded, and remanding her procedural due process claim to the district court).

²³² *Id.* at 819.

²³³ *See generally Witt*, 527 F.3d 806; *Cook*, 528 F.3d 42 (2008).

²³⁴ The district court declined such an undertaking because

none of the plaintiffs claims that the policy, if valid in general, was misapplied in his or her particular case to result in separation when a

The court reasoned that “the military’s effectiveness as a fighting force . . . is an exceedingly weighty interest and one that unquestionably surpasses the government interest that was at stake in *Lawrence*.”²³⁵ The court further reasoned that “[e]very as-applied challenge brought by a member of the armed forces against [DADT], at its core, implicates this interest.”²³⁶ As a result, all as-applied challenges must fail.²³⁷ The court relied upon the congressional record²³⁸ and the statutory language²³⁹ to determine that deference is warranted concerning the DADT policy. At the same time, the court conducted a balancing test on a broad social scale reminiscent of *Lawrence*, opining boldly that “where Congress has articulated a substantial government interest for a law, and where the challenges in question implicate that interest, judicial intrusion is simply not warranted.”²⁴⁰

The First Circuit’s dismissive treatment of all possible as-applied challenges to DADT is unpersuasive because Congress has made no findings with regard to any particular plaintiffs.²⁴¹ Thus, “deference to congressional findings does not make sense. There is nothing to defer to” with respect to any particular plaintiff.²⁴² Instead, the court’s attempt to conduct an as-applied analysis amounts to a judicial determination that no analysis should be conducted when Congress has recited a substantial interest as the basis for legislation.²⁴³

proper application of the policy would have allowed him or her to remain a service member. Rather, their objections, as articulated in the legal arguments in opposition to the motion to dismiss, are *that* the policy was applied, not *how* it was applied. This is classically a facial challenge to the statute, and their arguments will be evaluated with that understanding.

Cook v. Rumsfeld, 429 F. Supp. 2d 385, 390 (D. Mass. 2006) (emphasis in original).

²³⁵ Cook v. Gates, 528 F.3d. 42, 61 (2008) (emphasis added).

²³⁶ *Id.* at 60.

²³⁷ *Id.*

²³⁸ *Id.*

²³⁹ *Id.* (citing 10 U.S.C § 654(a)(12), (15) (2006)).

²⁴⁰ *Id.* (citing Rostker v. Goldberg, 453 U.S. 57, 68 (1982)).

²⁴¹ 10 U.S.C § 654(a) (2006).

²⁴² Lobsenz Telephone Interview, *supra* note 166.

²⁴³ *Cook*, 528 F.3d. at 56–60. Bizarrely, the First Circuit then claimed that “deference to Congressional judgment in this area does not mean abdication.” *Id.* at 60.

4. *The First Circuit's Equal Protection Analysis*

The First Circuit devoted substantially more attention to the question of equal protection than did the Ninth.²⁴⁴ The First Circuit distinguished the equal protection claim from the due process one, explaining that “[u]nlike the due process claim, which is premised on the constitutional protection afforded all citizens to engage in certain sexual conduct, the equal protection claim is based on the [DADT]’s differential treatment of homosexual military members versus heterosexual military members.”²⁴⁵ This distinction is critical because “*Lawrence* was a substantive due process decision that recognized a right in all adults, regardless of sexual orientation, to engage in certain intimate conduct.”²⁴⁶ Under equal protection, the relevant issues are the classification of persons and the basis for that classification.²⁴⁷ Where legislation targets a suspect class,²⁴⁸ heightened judicial scrutiny applies.²⁴⁹ Classifications aimed at “non-suspect classes are subject only to rational basis review.”²⁵⁰

The question for the equal protection claim before the First Circuit was whether homosexuals constitute a suspect class. The plaintiff’s equal protection claim was “that the district court erred by applying rational basis review because the Supreme Court’s decisions in *Romer v. Evans*, [citation omitted] and *Lawrence* mandate a more demanding standard.”²⁵¹ The court noted first that *Romer v. Evans* (*Romer*)²⁵²

invalidated, on equal protection grounds, a Colorado constitutional amendment which prohibited the enactment of any measure designed to protect individuals due to their sexual orientation. The Court analyzed the constitutionality of the amendment through the prism of rational basis, asking whether the classification bore “a rational relation to some legitimate

²⁴⁴ Seven hundred seventy three words, compared to the Ninth Circuit’s 116.

²⁴⁵ *Cook*, 528 F.3d. at 60.

²⁴⁶ *Id.* at 61 (citing *Lawrence*, 539 U.S. 558, 574–75 (2003)) (emphasis added).

²⁴⁷ *Romer v. Evans*, 517 U.S. 620, 633 (1996).

²⁴⁸ This has become a term of art in equal protection jurisprudence, originating with *Korematsu v. United States*, where the Court said “that all legal restrictions which curtail the civil rights of a single racial group are immediately suspect.” 323 U.S. 214, 215 (1944).

²⁴⁹ *Cook*, 528 F.3d. at 61.

²⁵⁰ *Id.*

²⁵¹ *Id.* (emphasis added).

²⁵² 517 U.S. 620, 633 (1996).

end.” Applying this standard, the Court concluded that the amendment was unconstitutional because the only possible justification for the amendment was “animosity toward the class of persons affected,” which does not constitute even “a legitimate governmental interest.”²⁵³

The First Circuit found nothing in *Romer* to indicate treatment of homosexual persons as a suspect class and found instructive its explicit use of a rational basis standard.²⁵⁴ The court also noted extensive case law from other circuits reaching the same conclusion.²⁵⁵

The First Circuit turned next to the question of whether *Lawrence* impacted the equal protection framework surrounding homosexual persons.²⁵⁶ Recognizing that “the *Lawrence* Court explicitly declined to base its ruling on equal protection principles, even though that issue was presented,”²⁵⁷ the First Circuit found no evidence that *Lawrence* conferred suspect classification status upon homosexual persons for purposes of equal protection.²⁵⁸ Absent specific language establishing such a classification, the First Circuit agreed with the district court²⁵⁹ that rational basis remains the applicable equal protection standard for legislation classifying persons on the basis of sexual orientation.²⁶⁰

Despite the plaintiffs’ argument that DADT should fail even the rational basis test,²⁶¹ the First Circuit closed its equal protection inquiry with the statement that, “Congress has put forward a non-animus based explanation for its decision to pass [DADT]. Given the substantial deference owed Congress’ assessment of the need for the legislation, [DADT] survives rational basis review.”²⁶²

²⁵³ *Cook*, 528 F.3d. at 61 (citation omitted) (quoting *Romer v. Evans*, 517 U.S. 631–35 (1996)).

²⁵⁴ *Id.*

²⁵⁵ *Id.* The court offered the following string citation referencing its sister circuits: “*Scarborough v. Morgan County Bd. of Educ.*, 470 F.3d 250, 261 (6th Cir. 2006); *Citizens for Equal Prot. v. Bruning*, 455 F.3d 859, 866 (8th Cir. 2006); *Johnson v. Johnson*, 385 F.3d 503, 532 (5th Cir. 2004); *Lofton*, 358 F.3d at 818; *Veney v. Wyche*, 293 F.3d 726, 731–32 (4th Cir. 2002); *Holmes*, 124 F.3d at 1132.”

²⁵⁶ *Id.*

²⁵⁷ *Id.* (citing *Lawrence v. Texas*, 539 U.S. 558, 574–75 (2003)) (emphasis added).

²⁵⁸ *Id.*

²⁵⁹ *Cook v. Rumsfeld*, 429 F. Supp. 2d 385, 405 (D. Mass. 2006).

²⁶⁰ *Cook*, 528 F.3d. at 61.

²⁶¹ *Id.*

²⁶² *Id.* at 62.

5. *The First Circuit's First Amendment Analysis*

Unlike the Ninth Circuit, the First Circuit addressed a First Amendment claim that DADT impinges on free speech.²⁶³ Under DADT, servicemembers' statements to the effect that they are homosexual or bisexual give rise to a rebuttable presumption that they will engage in prohibited conduct.²⁶⁴ This presumption, if un rebutted, is a basis for separation.²⁶⁵ The *Cook* plaintiffs attacked the rebuttable presumption with two arguments.²⁶⁶ First, they alleged that the presumption cannot be rebutted by persons whose sexual orientation is homosexual or bisexual, so that the effect of DADT is to punish the statement.²⁶⁷ Second, the plaintiffs alleged that even if a homosexual person could rebut the presumption, its existence forces "gay and lesbian service members to live in an environment that severely restricts and chills constitutionally protected speech."²⁶⁸

The *Cook* court rejected the first of these arguments on the grounds that "a person may say he or she is homosexual even though the person does not engage in, attempt to engage in, have a propensity to engage in, or intend to engage in homosexual acts."²⁶⁹ The court cited examples where servicemembers who had announced a homosexual orientation remained in the service because they indicated they would not engage in prohibited conduct.²⁷⁰ The plaintiffs' claim that the existence of the presumption chills protected speech failed because "the member's speech continues to have only evidentiary significance in making this conduct-focused determination."²⁷¹ The court acknowledged that DADT "does

²⁶³ *Id.* Major Witt did not raise, and the Ninth Circuit did not discuss, a free speech claim under the First Amendment. See generally Witt v. Dep't of the Air Force, 527 F.3d 806, (2008) and Brief of Appellant-Petitioner, Witt v. Dep't of the Air Force, No. 06-35644 (9th Cir. Oct. 16, 2006) (discussing the First Amendment only in historical context on the matter of freedom of association).

²⁶⁴ 10 U.S.C. § 654(b)(2) (2006).

²⁶⁵ *Id.*

²⁶⁶ *Cook*, 528 F.3d. at 64.

²⁶⁷ *Id.*

²⁶⁸ *Id.*

²⁶⁹ *Id.*

²⁷⁰ *Id.* ("One female Naval officer admitted to her homosexuality but submitted a statement, in which she stated, *inter alia*, that she understands the rules against homosexual conduct and intended to obey those rules. Another female Naval officer stated that she was a lesbian but that the statement 'in no way, was meant to imply [] any propensity or intent or desire to engage in prohibited conduct.'") (citing Holmes v. Cal. Army Nat'l Guard 124 F.3d 1126, 1136 (1997)).

²⁷¹ *Id.* at 62.

affect the right of military members to express their sexual orientation by establishing the possibility of adverse consequences” for declaring a homosexual orientation,²⁷² but noted that any time the law “prohibits certain acts, it necessarily chills speech that constitutes evidence of the acts. A regulation directed at acts thus inevitably restricts a certain type of speech; this policy is no exception. But effects of this variety do not establish a content-based restriction of speech.”²⁷³

In his expository dissent, Judge Saris concluded that the “plaintiffs have made sufficient allegations that the burden that the statement presumption places on speech is greater than is essential, particularly in nonmilitary settings off-base and off-duty.”²⁷⁴ He reached this conclusion because DADT’s “statement presumption chills individual service members from discussing homosexuality both privately and publicly even when they have no intent to engage in prohibited homosexual conduct.”²⁷⁵ Although the military enjoys the widest latitude in controlling speech,²⁷⁶ Judge Saris concluded that the rebuttable presumption provision, which “applies ‘24 hours [a] day,’ and applies even to speech made ‘off base’ and/or ‘off duty,’”²⁷⁷ and in the most private contexts, “such as confiding in a friend or words within a letter from a friend or family member,”²⁷⁸ is more expansive than necessary to advance the stated governmental interest.²⁷⁹

B. The Crystal Ball

This section attempts to predict the outcome of a potential judicial review of DADT by the Supreme Court. It is noteworthy that both circuit courts offer a tempting common ground concerning DADT under post-*Lawrence* due process—both courts subjected DADT to an intermediate level of scrutiny. In the event the Supreme Court were to review either or both of the circuit cases, it is likely to agree with the two

²⁷² *Id.* at 63.

²⁷³ *Id.* (quoting *Thomasson v. Perry*, 80 F.3d 915 (4th Cir. 1996)).

²⁷⁴ *Id.* at 74.

²⁷⁵ *Id.*

²⁷⁶ *Id.* at 73 (“See e.g., *Goldman*, 475 U.S. at 507-10 (affording deference to regulation that prevented soldiers from wearing yarmulkes while on duty and in uniform); *Brown v. Glines*, 444 U.S. 348, 354-55 (1980) (affording deference to regulation that prevented soldiers from circulating petitions on air force bases).”).

²⁷⁷ *Id.* at 74 (quoting 10 U.S.C. § 654(a)(9)-(11) (2006)).

²⁷⁸ *Id.*

²⁷⁹ *Id.* See generally *Wayte v. United States*, 470 U.S. 598, 611 (1985).

circuits that the liberty interest in private, adult, consensual sexual intimacy is protected under due process as interpreted by the circuits and consistent with *Lawrence*, and that the protection afforded this liberty interest subjects statutory efforts to infringe upon it to a higher than rational basis review. Like the circuit courts, the Supreme Court would likely agree that the protection of the liberty interest does not require application of strict scrutiny.²⁸⁰ Such findings would offer the Court flexibility in addressing the constitutionality of DADT, while avoiding less developed areas of equal protection and First Amendment law as they apply to homosexuality in the military.

Equal protection arguments are unlikely to form the basis of a Supreme Court ruling on DADT. The circuit court decisions do not undermine the rational basis standard for classification of homosexual persons as a group under equal protection, and this standard of review appears unlikely to change as a result. Although the equal protection analyses presented by the circuit courts are unsatisfying, their contrast with careful and detailed due process discussions illustrates the comparatively little weight equal protection carries in the arena of homosexuality as a classification in our society. The DADT policy affects primarily the military—a small slice of the larger American society, and one which is widely considered jurisprudentially distinct.²⁸¹ A successful challenge to the equal protection status of homosexual persons would more likely arise from circumstances more broadly applicable than gays in the military.²⁸² Finally, DADT may not be an ideal vehicle to challenge the equal protection status quo with regard to sexual orientation because DADT explicitly addresses acts, not status.²⁸³

The Court would likely find no protection for speech of evidentiary character under the First Amendment, though such an approach can be conceived and may contribute to judicial intervention. After *Lawrence*

²⁸⁰ E-mail from Shaun Martin, Law Professor, University of San Diego School of Law (Oct. 9, 2008, 14:09:31 EST) (on file with author) (noting that the Supreme Court would “be hesitant to employ straightforward strict scrutiny, even after *Lawrence* and *Romer*”).

²⁸¹ See *Parker v. Levy*, 417 U.S. 733, 755 (1974) (“Congress is permitted to legislate both with greater breadth and with greater flexibility when the statute governs military society.”); *Burns v. Wilson*, 346 U.S. 137, 140 (1953) (“Military law . . . is a jurisprudence which exists separate and apart from the law which governs in our federal judicial establishment.”). See generally Chief Justice Earl Warren, *The Bill of Rights and the Military*, 37 N.Y.U. L. REV. 181, 197 (1962) (“[T]he Court has viewed the separation and subordination of the military establishment as a compelling principle.”).

²⁸² See Lobsenz Telephone Interview, *supra* note 166.

²⁸³ 10 U.S.C. § 654(b)(1) (2006).

and *Marcum*, DADT “operates as an evidentiary mechanism for the military to target conduct that, according to the military’s own courts, can no longer be criminalized.”²⁸⁴ It can be argued that the real reason for the policy is that “the military leadership believes its rank and file could not stomach” the idea of homosexuality among military members—a paradigm of prohibited viewpoint discrimination²⁸⁵ under the First Amendment.²⁸⁶ These concerns, coupled with the issues raised by Judge Saris in his dissent,²⁸⁷ raise significant questions about the constitutionality of DADT as it is currently administered. Even if the Court were to agree that the rebuttable presumption based upon a statement of homosexuality violates the First Amendment, it is not necessary to scrap the entire policy on First Amendment grounds. A *Witt*-style requirement that the Government show case-specific evidence of military harm from the specific homosexual acts alleged would undermine the application of the presumption as an independent basis for separation. Where the Court can avoid a constitutional issue, it will do so as a matter of policy.²⁸⁸

A due process analysis presents the greatest threat to DADT. Remaining within the common ground of the circuit courts’ treatment of due process would provide a principled foundation for the Court to address the application of DADT without overturning it. This approach would also provide the Court leeway to determine the degree of its deference to Congress on military matters—it could insist on a case-by-case application of congressional intent a la *Witt*, or it could follow *Cook* and abdicate. Finally, the Court could use the circuit courts’ consensus that higher than rational basis is required after *Lawrence* as a springboard to overturn DADT on due process grounds. Each possibility is examined in turn.

1. Option 1—The policy will survive constitutional muster under a heightened scrutiny standard requiring the Government to show a

²⁸⁴ Shannon Gilreath, *Sexually Speaking: “Don’t Ask, Don’t Tell” and the First Amendment after Lawrence v. Texas*, 14 DUKE J. GENDER L. & POL’Y 953, 958 (May, 2007).

²⁸⁵ Viewpoint discrimination is Government action stifling “speech on account of its message, or that requires the utterance of a particular message favored by the Government.” *Turner Broad. v. FCC*, 512 U.S. 622 (1994).

²⁸⁶ Gilreath, *supra* note 284, at 958.

²⁸⁷ *Cook v. Gates*, 528 F.3d 42, 65 (2008) (Saris, J., dissenting).

²⁸⁸ GUNTHER & SULLIVAN, *supra* note 36, at 29.

specific unit impact in the particular case of the Soldier to be separated, effectively creating a regime where homosexual acts resulting in actual disruption can form a basis for separation. This is likely.

Although the Court could create an altogether new framework of analysis, or defer entirely to Congress as in *Cook*, it is likely the Court will adopt the *Sell* factors as applied in *Witt*. This outcome is likely because the *Sell* factors offer a persuasive and convenient framework grounded in Supreme Court precedent. The Court in *Sell* created a balancing test specifically tailored to weigh private liberty interests against the needs of the Government. Rejection of that test in the context of private sexual activity would require the court to address why sexual activity, and in particular homosexual activity, should be treated differently. The Court is unlikely to invite criticism by attempting to carve out special legal rules for homosexuals when more facially neutral means are available. Perhaps most importantly, the *Sell* factors will not commit the Court to a specific course of action regarding the facial validity of DADT. By invoking the *Sell* factors the Court can address the constitutional difficulties of DADT without striking the statute.

The *Sell* factors would limit, but not preclude, the military's application of DADT. In cases where the private sexual practices of a military member do not adversely impact the "high standards of morale, good order and discipline, and unit cohesion,"²⁸⁹ commanders generally have little incentive to pursue separation under DADT. In cases where the conduct causes disruption, commanders would need only to document the effects in consultation with their assigned legal advisors. Documenting adverse unit impact is a routine part of administrative separations under other provisions²⁹⁰ and is unlikely to present a significant administrative burden. Commanders could also allow reassignment to another unit in appropriate cases. Thus, application of the *Sell* test will have a *de minimis* impact on the military in cases where Congress's concerns of military effectiveness are implicated.

2. *Option 2—The Supreme Court, while upholding the Witt and Cook determinations concerning the Lawrence liberty interest, will*

²⁸⁹ 10 U.S.C. § 654(a)(15) (2006).

²⁹⁰ See, e.g., U.S. DEP'T OF ARMY, REG. 635-200, ENLISTED SEPARATIONS paras. 13 (unsatisfactory performance), 14-12b (pattern of misconduct) (6 June 2005).

follow Cook and show deference to the point of abdication to Congress's findings. This is less likely.

If the Supreme Court were to adopt the First Circuit's approach, the military would carry on with business as usual. This outcome is unlikely because, as even the *Cook* Court admitted,²⁹¹ "deference to [c]ongressional judgment in this area does not mean abdication."²⁹²

The First Circuit found significant depth of concern reflected in the congressional record, as explained in *Cook*, over matters of privacy, liberty, and morality concerning private sexual conduct, and the application of social values in the military context specifically.²⁹³ As the First Circuit explained, "[t]he circumstances surrounding [DADT]'s passage lead to the firm conclusion that Congress and the Executive studied the issues intensely and from many angles, including by considering the constitutional rights of gay and lesbian service members."²⁹⁴ Deference to congressional determinations is rooted in the Constitution, which grants Congress the power to "raise and support armies . . . and [t]o make all Laws which shall be necessary and proper" for that purpose.²⁹⁵ The Supreme "Court has described this power as 'broad and sweeping'"²⁹⁶ and professed inability to intelligently address military matters, claiming that

[i]t is difficult to conceive of an area of governmental activity in which courts have less competence. The complex, subtle, and professional decisions as to the composition, training, equipping and control of a military force are essentially professional military judgments, subject always to civilian control of the Legislative and Executive Branches.²⁹⁷

²⁹¹ This admission was made while announcing a policy of blanket abdication. *Cook*, 528 F.3d at 60.

²⁹² *Id.*

²⁹³ *Id.* at 58–60.

²⁹⁴ *Id.* at 59.

²⁹⁵ U.S. CONST. art. I, § 8, cls. 12–14.

²⁹⁶ *Cook*, 528 F.3d at 59 (quoting *United States v. O'Brien*, 391 U.S. 367, 377 (1968)).

²⁹⁷ *Id.* (quoting *O'Brien*, 391 U.S. at 377).

This facially strong argument for blanket deference fails for three primary reasons.²⁹⁸ First, taken to its logical end, *Cook*'s reasoning would unfetter military affairs from constitutional restraints. This is not the law, for the Supreme Court has explained that deference does not free Congress "to disregard the Constitution when it acts in the area of military affairs. In that area, as any other, Congress remains subject to the limitations of the Due Process Clause."²⁹⁹

Second, DADT undermines the legislative process because it prohibits the class of persons directly affected by the policy, homosexual military personnel, from open participation in the public discussion.³⁰⁰ Legislative representatives are unlikely to hear from constituent military members affected by DADT, while constituents on the other side of the debate may speak freely. As Professor Shannon Gilreath³⁰¹ observed,

the only soldiers who may speak in favor of the ability of gays and lesbians to live authentic lives while serving their country are straight soldiers, or gays who are secreting their authentic selves. It is a curious debate indeed when the only people prohibited from debating are the victims of the policy the debate addresses.³⁰²

This silent constituency may be significant, with claims that up to "65,000 gay men and lesbians now serve in the American armed forces and that there are more than one million gay veterans."³⁰³ Where they are not meaningfully represented in the legislative debate, the federal courts may be uniquely qualified to intervene because the courts hear directly from active duty military personnel when they contest their separations through litigation.

²⁹⁸ The fact that Congress remained substantially divided on DADT at the time of this writing does not undermine deference, since the issue is deference to the findings recited in the Act and not deference to a subjective perception of the mood of Congress at a particular moment.

²⁹⁹ *Rostker v. Goldberg*, 453 U.S. 57, 67 (1981); see also Warren, *supra* note 281, at 188 ("[O]ur citizens in uniform may not be stripped of basic rights simply because they have doffed their civilian clothes.").

³⁰⁰ Gilreath, *supra* note 284, at 961.

³⁰¹ Assistant Director for the International Graduate Program and Adjunct Professor of Law at Wake Forest University.

³⁰² Gilreath, *supra* note 284, at 962.

³⁰³ Thom Shanker & Patrick Healy, *A New Push to Roll Back 'Don't Ask, Don't Tell'*, N.Y. TIMES, Nov. 30, 2007, available at <http://www.nytimes.com/2007/11/30/us/30/military.html>.

Third, the nexus between military effectiveness and the conduct proscribed under DADT is problematic. In order to rest on naked deference regarding DADT, the Court would have to explain why separation of servicemembers based upon private sexual conduct is a military matter rather than a legal one. This would require a connection between private sexual activity and military effectiveness—a connection which, if manifested in form of sexual assault or harassment, would likely violate a number of uncontroversial criminal statutes addressing sexual misconduct.³⁰⁴ Where the law already addresses sexual misconduct in wide and gender-neutral terms, to include most conceivable sexual activity in the military workplace,³⁰⁵ it is difficult to conceive of facts where sexual orientation could disrupt the military environment without triggering existing criminal enforcement mechanisms.

Congress attempted to bridge this logical gap with the finding that “presence in the armed forces of persons who demonstrate a propensity or intent to engage in homosexual acts would create an unacceptable risk to the high standards of morale, good order and discipline, and unit cohesion that are the essence of military capability.”³⁰⁶ This conclusory statement fails to show a causal relationship between the private sexual conduct and military effectiveness,³⁰⁷ instead relying implicitly on the assumption that personal bias within the military ranks will create friction where homosexual, rather than heterosexual, conduct becomes known. Since “[p]rivate biases may be outside the reach of the law, but the law cannot, directly or indirectly, give them effect,”³⁰⁸ the Court would likely demand a more explicit connection between private sexual conduct and military effectiveness.

3. *Option 3—DADT will fail judicial review. This is unlikely.*

Opposite abdication on the scale of judicial activism is wholesale destruction of legislation by the judiciary. The Court exercises its power

³⁰⁴ See, e.g., MCM, *supra* note 100, pt. IV, ¶¶ 45, 51.

³⁰⁵ *Id.*; AR 600-20, *supra* note 77, ch. 7 (Prevention of Sexual Harassment).

³⁰⁶ 10 U.S.C. § 654(a)(15) (2006).

³⁰⁷ Gilreath, *supra* note 284, at 972 (“The easiest way to see that irrationality is to replace the argument’s reference to ‘gays’ with reference to ‘blacks.’ This requires no great feat of imagination, because it was precisely the argument made in resistance to racial integration of the military in the 1940s.”).

³⁰⁸ *Palmore v. Sidoti*, 466 U.S. 429, 433 (1984).

of judicial review with great care, applying a policy of strict necessity,³⁰⁹ and “has frequently called attention to the ‘great gravity and delicacy’ of its function in passing upon the validity of an act of Congress.”³¹⁰ This reluctance to leap to constitutional activism means that, even when legislation is constitutionally problematic, the Supreme Court will seek a way to interpret the statute in a way that does not violate the Constitution.³¹¹

Although the circuit courts did not agree on their application of heightened scrutiny to DADT, they both focus substantially on its application rather than its facial validity. *Witt*, in particular, focused explicitly on the application of Congress’s legislation to the particular plaintiff. Its instructions on remand are essentially procedural steps for compliance with the act.³¹² This approach would offer the Supreme Court a method of analysis that stops short of striking the statute. Where such an alternative exists and especially, as here, where lower courts have laid a foundation, the Supreme Court is unlikely to apply judicial review more broadly.

It is unlikely that the Court will apply strict scrutiny to DADT. While equal protection,³¹³ the First Amendment,³¹⁴ and due process all

³⁰⁹ GUNTHER & SULLIVAN, *supra* note 36, at 29.

³¹⁰ *Ashwander v. TVA*, 297 U.S. 288, 345 (1936) (Brandeis, J., concurring).

³¹¹ *Id.* at 348.

³¹² *Witt v. Dep’t of the Air Force*, 527 F.3d 806, 821 (2008).

The Air Force attempts to justify the policy by relying on congressional findings regarding “unit cohesion” and the like, but that does not go to whether the application of DADT specifically to Major Witt significantly furthers the government’s interest and whether less intrusive means would achieve substantially the government’s interest. Remand therefore is required for the district court to develop the record on Major Witt’s substantive due process claim. Only then can DADT be measured against the appropriate constitutional standard.

Id.

³¹³ *Id.* at 824 (2008) (Canby, J., dissenting) (arguing that DADT is subject to strict scrutiny under equal protection because homosexuals are a suspect class and the *Lawrence* liberty interest is a matter of the equality of homosexual persons).

³¹⁴ *E.g.*, Gilreath, *supra* note 284, at 967–68.

[S]trict scrutiny emerges as the appropriate evaluative standard for the government’s regulations of expression via “Don’t Ask, Don’t Tell.” Governmental regulation of expressive conduct warrants strict

suggest that institutional discrimination against homosexual persons, or private sexual relationships, should be subject to strict scrutiny, the Court had the opportunity to set that standard in *Lawrence*. It did not.³¹⁵ Where the lower courts have articulated an intermediate scrutiny consistent with *Lawrence*, the Court will not likely risk “the respect accorded to the judgments of the Court and to the stability of the law”³¹⁶ by undermining them.

Application of strict scrutiny, while unlikely, is not impossible. Since *Lawrence* was silent on the standard of review,³¹⁷ it left open the possibility of clarifying the appropriate standard in light of future developments in law and society. The Court expressed its concern that “*Bowers* itself causes uncertainty, for the precedents before and after its issuance contradict its central holding.”³¹⁸ *Lawrence* has likewise caused confusion.³¹⁹ The Court could determine that the circuit court decisions have made ripe the question of the standard of review required under *Lawrence*, and that the standard is strict scrutiny. If the Court applies strict scrutiny to DADT, it will almost certainly overturn it.³²⁰

Should it do so, the military will remain well-positioned to address acts of sexual conduct, homosexual or heterosexual, that adversely impact military effectiveness. Sexual tension in the workplace is a form of hostile work environment prohibited by military regulations.³²¹ Contributing to such an environment is punishable under the Uniform Code of Military Justice.³²² Military commanders’ remedies for non-criminal sexual speech or behavior in the workplace would no longer vary with the sexual orientation character of the underlying acts but

scrutiny when (1) the regulation of speech or conduct targets the message that the speech or conduct communicates to others and (2) similar expression is regulated differently based on the communicated viewpoint of the speaker.

Id.

³¹⁵ *Lawrence*, 539 U.S. 558 (2003); *Witt*, 527 F.3d at 818; *Cook*, 528 F.3d at 54.

³¹⁶ *Lawrence*, 539 U.S. at 577.

³¹⁷ *Witt*, 527 F.3d at 814.

³¹⁸ *Lawrence*, 539 U.S. at 577.

³¹⁹ See generally *e.g.*, *Witt*, 527 F.3d 806; *Cook*, 528 F.3d 42; *United States v. Marcum*, 60 M.J. 198, 206–07 (C.A.A.F. 2004); *supra* Part II.D.

³²⁰ See generally *e.g.*, *Cook*, 528 F.3d at 65; *Witt*, 527 F.3d at 822 (Canby, J., dissenting); *supra* note 197.

³²¹ See, *e.g.*, AR 600-20, *supra* note 77, ch. 7 (Prevention of Sexual Harassment), MCM, *supra* note 100, pt. IV, ¶ 16 (criminalizing violation of certain regulations, including AR 600-20).

³²² MCM, *supra* note 100, pt. IV, ¶¶ 16, 17.

would instead rely upon existing gender-neutral enforcement mechanisms. Aggressive implementation of military equal opportunity programs would enable military leaders to prevent discomfort with homosexuality from impacting unit effectiveness.³²³ In addition, the military disciplinary structure is uniquely suited to suppressing discriminatory attitudes among servicemembers, as illustrated by its spectacular, albeit initially difficult, success with racial integration in 1948.³²⁴

IV. Conclusion

Although “[l]awyers and courts alike puzzle over the different interpretations”³²⁵ of *Lawrence* for DADT, the *Witt* court’s analysis presents the most attractive, persuasive and convenient resolution of the current tension between DADT and society’s evolving expectations of due process. Should the Supreme Court review the matter, it would probably subject DADT to a higher than rational basis standard of review, but stop short of strict scrutiny. As a result, the policy would likely survive in a weakened form, where the Government must bring case specific evidence of adverse unit impact resulting from the homosexual acts in question. From a practical standpoint, military commanders and attorneys involved in the implementation of DADT should prepare to consider each case in terms of adverse unit impact and be prepared to document any such impact prior to separating personnel under DADT.

³²³ See, e.g., AR 600-20, *supra* note 77, ch. 6 (The Equal Opportunity Program in the Army).

The Equal Opportunity (EO) Program formulates, directs, and sustains a comprehensive effort to maximize human potential and to ensure fair treatment for all persons based solely on merit, fitness, and capability in support of readiness. EO philosophy is based on fairness, justice, and equity. Commanders are responsible for sustaining a positive EO climate within their units.

Id. para 6-1.

³²⁴ See generally MORRIS J. MACGREGOR, JR., INTEGRATION OF THE ARMED FORCES 1940–1965 (1985).

³²⁵ Persky, *supra* note 62.

Appendix

DADT Full Text

UNITED STATES CODE SERVICE
Copyright © 2008 Matthew Bender & Company, Inc.
a member of the LexisNexis Group.
All rights reserved

*** CURRENT THROUGH PL 110-353, APPROVED 10/7/2008 ***
*** WITH GAPS OF 110-343, 110-344, 110-346 and 110-351 ***

TITLE 10. ARMED FORCES
SUBTITLE A. GENERAL MILITARY LAW
PART II. PERSONNEL
CHAPTER 37. GENERAL SERVICE REQUIREMENTS

10 USCS § 654

§ 654. Policy concerning homosexuality in the armed forces

(a) Findings. Congress makes the following findings:

(1) Section 8 of article I of the Constitution of the United States commits exclusively to the Congress the powers to raise and support armies, provide and maintain a Navy, and make rules for the government and regulation of the land and naval forces.

(2) There is no constitutional right to serve in the armed forces.

(3) Pursuant to the powers conferred by section 8 of article I of the Constitution of the United States, it lies within the discretion of the Congress to establish qualifications for and conditions of service in the armed forces.

(4) The primary purpose of the armed forces is to prepare for and to prevail in combat should the need arise.

(5) The conduct of military operations requires members of the armed forces to make extraordinary sacrifices, including the ultimate sacrifice, in order to provide for the common defense.

(6) Success in combat requires military units that are characterized by high morale, good order and discipline, and unit cohesion.

(7) One of the most critical elements in combat capability is unit cohesion, that is, the bonds of trust among individual service members

that make the combat effectiveness of a military unit greater than the sum of the combat effectiveness of the individual unit members.

(8) Military life is fundamentally different from civilian life in that--

(A) the extraordinary responsibilities of the armed forces, the unique conditions of military service, and the critical role of unit cohesion, require that the military community, while subject to civilian control, exist as a specialized society; and

(B) the military society is characterized by its own laws, rules, customs, and traditions, including numerous restrictions on personal behavior, that would not be acceptable in civilian society.

(9) The standards of conduct for members of the armed forces regulate a member's life for 24 hours each day beginning at the moment the member enters military status and not ending until that person is discharged or otherwise separated from the armed forces.

(10) Those standards of conduct, including the Uniform Code of Military Justice, apply to a member of the armed forces at all times that the member has a military status, whether the member is on base or off base, and whether the member is on duty or off duty.

(11) The pervasive application of the standards of conduct is necessary because members of the armed forces must be ready at all times for worldwide deployment to a combat environment.

(12) The worldwide deployment of United States military forces, the international responsibilities of the United States, and the potential for involvement of the armed forces in actual combat routinely make it necessary for members of the armed forces involuntarily to accept living conditions and working conditions that are often spartan, primitive, and characterized by forced intimacy with little or no privacy.

(13) The prohibition against homosexual conduct is a longstanding element of military law that continues to be necessary in the unique circumstances of military service.

(14) The armed forces must maintain personnel policies that exclude persons whose presence in the armed forces would create an unacceptable risk to the armed forces' high standards of morale, good order and discipline, and unit cohesion that are the essence of military capability.

(15) The presence in the armed forces of persons who demonstrate a propensity or intent to engage in homosexual acts would create an unacceptable risk to the high standards of morale, good order and discipline, and unit cohesion that are the essence of military capability.

(b) Policy. A member of the armed forces shall be separated from the armed forces under regulations prescribed by the Secretary of Defense if

one or more of the following findings is made and approved in accordance with procedures set forth in such regulations:

(1) That the member has engaged in, attempted to engage in, or solicited another to engage in a homosexual act or acts unless there are further findings, made and approved in accordance with procedures set forth in such regulations, that the member has demonstrated that--

(A) such conduct is a departure from the member's usual and customary behavior;

(B) such conduct, under all the circumstances, is unlikely to recur;

(C) such conduct was not accomplished by use of force, coercion, or intimidation;

(D) under the particular circumstances of the case, the member's continued presence in the armed forces is consistent with the interests of the armed forces in proper discipline, good order, and morale; and

(E) the member does not have a propensity or intent to engage in homosexual acts.

(2) That the member has stated that he or she is a homosexual or bisexual, or words to that effect, unless there is a further finding, made and approved in accordance with procedures set forth in the regulations, that the member has demonstrated that he or she is not a person who engages in, attempts to engage in, has a propensity to engage in, or intends to engage in homosexual acts.

(3) That the member has married or attempted to marry a person known to be of the same biological sex.

(c) Entry standards and documents.

(1) The Secretary of Defense shall ensure that the standards for enlistment and appointment of members of the armed forces reflect the policies set forth in subsection (b).

(2) The documents used to effectuate the enlistment or appointment of a person as a member of the armed forces shall set forth the provisions of subsection (b).

(d) Required briefings. The briefings that members of the armed forces receive upon entry into the armed forces and periodically thereafter under section 937 of this title [10 USCS § 937] (article 137 of the Uniform Code of Military Justice) shall include a detailed explanation of the applicable laws and regulations governing sexual conduct by members of the armed forces, including the policies prescribed under subsection (b).

(e) Rule of construction. Nothing in subsection (b) shall be construed to require that a member of the armed forces be processed for separation from the armed forces when a determination is made in accordance with regulations prescribed by the Secretary of Defense that--

(1) the member engaged in conduct or made statements for the purpose of avoiding or terminating military service; and

(2) separation of the member would not be in the best interest of the armed forces.

(f) Definitions. In this section:

(1) The term "homosexual" means a person, regardless of sex, who engages in, attempts to engage in, has a propensity to engage in, or intends to engage in homosexual acts, and includes the terms "gay" and "lesbian".

(2) The term "bisexual" means a person who engages in, attempts to engage in, has a propensity to engage in, or intends to engage in homosexual and heterosexual acts.

(3) The term "homosexual act" means--

(A) any bodily contact, actively undertaken or passively permitted, between members of the same sex for the purpose of satisfying sexual desires; and

(B) any bodily contact which a reasonable person would understand to demonstrate a propensity or intent to engage in an act described in subparagraph (A).

History:

(Added Nov. 30, 1993, P.L. 103-160, Div A, Title V, Subtitle G, § 571(a)(1), 107 Stat. 1670.)

History; Ancillary Laws and Directives:

Other provisions

Regulations. Act Nov. 30, 1993, P.L. 103-160, Div A, Title V, Subtitle G, § 571(b), 107 Stat. 1673, provides: "Not later than 90 days after the date of enactment of this Act, the Secretary of Defense shall revise Department of Defense regulations, and issue such new regulations as may be necessary, to implement section 654 of title 10, United States Code, as added by subsection (a)."

Savings provision. Act Nov. 30, 1993, P.L. 103-160, Div A, Title V, Subtitle G, § 571(c), 107 Stat. 1673, provides: “Nothing in this section or section 654 of title 10, United States Code, as added by subsection (a), may be construed to invalidate any inquiry, investigation, administrative action or proceeding, court-martial, or judicial proceeding conducted before the effective date of regulations issued by the Secretary of Defense to implement such section 654.”.

Sense of Congress. Act Nov. 30, 1993, P.L. 103-160, Div A, Title V, Subtitle G, § 571(d), 107 Stat. 1673, provides: “It is the sense of Congress that--

“(1) the suspension of questioning concerning homosexuality as part of the processing of individuals for accession into the Armed Forces under the interim policy of January 29, 1993, should be continued, but the Secretary of Defense may reinstate that questioning with such questions or such revised questions as he considers appropriate if the Secretary determines that it is necessary to do so in order to effectuate the policy set forth in section 654 of title 10, United States Code, as added by subsection (a); and

“(2) the Secretary of Defense should consider issuing guidance governing the circumstances under which members of the Armed Forces questioned about homosexuality for administrative purposes should be afforded warnings similar to the warnings under section 831(b) of title 10, United States Code (article 31(b) of the Uniform Code of Military Justice).”.

Notes:

Am Jur:

16B Am Jur 2d, Constitutional Law § 850.

Labor and Employment:

10 Larson on Employment Discrimination, ch 168, Discrimination Based on Sexual Orientation § 168.07.

4 Labor and Employment Law (Matthew Bender), ch 127, Discrimination Based on Sexual Orientation § 127.07.

Annotations:

Federal and State Constitutional Provisions as Prohibiting Discrimination in Employment on Basis of Gay, Lesbian, or Bisexual Sexual Orientation or Conduct. 96 ALR5th 391.

Interpretive Notes and Decisions:

1. Generally
2. Constitutionality
3. Standing
4. Injunction
5. Application

1. Generally

In deciding to issue preliminary injunctions in case brought by six gay or lesbian members of armed forces challenging constitutionality of law embodying “don’t ask, don’t tell” policy, district court should have required plaintiffs to prove likelihood of success on merits rather than only “serious questions going to merits,” since governmental policies implemented through legislation or regulations developed through presumptively democratic processes are entitled to higher degree of deference and should not be enjoined lightly. *Able v United States* (1995, CA2 NY) 44 F3d 128, 67 BNA FEP Cas 1095, 65 CCH EPD P 43399.

Claim of members of United States Armed Services, alleging that they are homosexuals and that Services’ policy and regulations as to homosexuals violated their right to equal protection, is not dismissed, because although government is entitled to deference where constitutional rights of service members are implicated, plaintiffs are entitled to attempt to prove that findings underlying statute are based solely on prejudice or fear of prejudice, or otherwise that there is no rational relationship between statute’s classifications of gay and lesbian service members and legitimate government purpose. *Able v United States* (1994, ED NY) 863 F Supp 112, app den (1994, ED NY) 870 F Supp 468, 67 BNA FEP Cas 1092, remanded (1995, CA2 NY) 44 F3d 128, 67 BNA FEP Cas 1095, 65 CCH EPD P 43399.

2. Constitutionality

In action by 6 self-identified homosexual members of Armed Services, court declares 10 USCS § 654 constitutional, where statute prohibits statement “I am homosexual or have homosexual propensities,” because § 654(b)(2) advances a substantial governmental interest and restricts

speech no more than is reasonably necessary. *Able v United States* (1996, CA2 NY) 88 F3d 1280, 71 BNA FEP Cas 419, 68 CCH EPD P 44233, on remand, injunction gr (1997, ED NY) 968 F Supp 850, 71 CCH EPD P 44999, revd on other grounds (1998, CA2 NY) 155 F3d 628, 74 CCH EPD P 45501.

Discharge of servicemember who stated that he was homosexual and had engaged in and intended to continue to engage in homosexual acts did not violate servicemember's right to equal protection since his discharge under "acts" prong of statute is constitutionally permissible because relationship between Navy's mission and its policy on homosexual acts renders distinction between acts and status rational; nor did his discharge violate his First Amendment right to free speech since his statements were used as evidence, not as reason for discharge. *Philips v Perry* (1997, CA9 Wash) 106 F3d 1420, 97 CDOS 1038, 97 Daily Journal DAR 1551, 70 CCH EPD P 44721, amd (1997, CA9 Wash) 97 CDOS 2848, 97 Daily Journal DAR 5031.

Statute setting forth policy on homosexuals in military, and its implementing regulations, are constitutionally valid; both circuit precedent and that from other circuits establishes that military has legitimate interest in discharging service members on account of homosexual conduct in order to maintain effective armed forces. *Holmes v California Army Nat'l Guard* (1997, CA9 Cal) 124 F3d 1126, 97 CDOS 7165, 97 Daily Journal DAR 11571, 71 CCH EPD P 45000, reh, en banc, den (1998, CA9) 155 F3d 1049, 98 CDOS 7548, 98 Daily Journal DAR 10518, 74 CCH EPD P 45513 and cert den (1999) 525 US 1067, 119 S Ct 794, 142 L Ed 2d 657.

Statute mandating termination of service of member of armed forces for engaging in homosexual conduct does not violate equal protection clause of Fifth Amendment; government justifications rationally related prohibition to goals of promoting unit cohesion, enhancing privacy and reducing sexual tension. *Able v United States* (1998, CA2 NY) 155 F3d 628, 74 CCH EPD P 45501.

10 USCS § 654 does not constitute unconstitutional bill of attainder, where statute creates rebuttable presumption that military officer who states he or she is homosexual has propensity to engage in homosexual acts, but policy expressed by statute does not fall within historical meaning of legislative punishment, since under policy homosexuals are not barred from military simply because they are homosexuals, and

statute leaves open possibility of qualifying for continued military service when homosexual overcomes presumption that he or she does engage in, attempts to engage in, has a propensity to engage in, or intends to engage in homosexual acts. *Richenberg v Perry* (1995, DC Neb) 909 F Supp 1303, 68 CCH EPD P 44121, injunction den (1995, CA8 Neb) 73 F3d 172, 69 BNA FEP Cas 883 and affd (1996, CA8 Neb) 97 F3d 256, 68 CCH EPD P 44259, reh, en banc, den (1997, CA8) 1997 US App LEXIS 1040 and cert den (1997) 522 US 807, 118 S Ct 45, 139 L Ed 2d 12.

Military's "Don't Ask, Don't Tell" policy, implemented under 10 USCS § 654, which discharges homosexuals from military service who admit to being homosexuals, did not substantially further government's interest in preventing unit polarization as required under heightened scrutiny standard of First Amendment, where silent homosexuals were allowed to serve, even though they still could read gay literature, frequent gay bars, march in gay rights parades, and vociferously advocate right of gays to serve, thus causing same degree of debate, unrest, and polarization as that caused by person who admitted homosexuality. *Thorne v United States DOD* (1996, ED Va) 916 F Supp 1358, 71 BNA FEP Cas 565, summary judgment gr, dismd (1996, ED Va) 945 F Supp 924 and affd without op (1998, CA4 Va) 139 F3d 893, reported in full (1998, CA4 Va) 1998 US App LEXIS 6904 and cert den (1998) 525 US 947, 142 L Ed 2d 307, 119 S Ct 371.

Challenge by 12 former service members to constitutionality of 10 USCS § 654, "Don't Ask/Don't Tell" policy on homosexuality in armed services, was dismissed for failure to state claim upon which relief could be granted because rational basis standard of review applied where right advanced by service members was neither fundamental nor involved suspect class, and Congress' goal of maintaining high standards of morale, good order, and discipline in military was rational in sense necessary to withstand constitutional challenge and sufficient to end substantive due process review and to foreclose most of equal protection challenges. *Cook v Rumsfeld* (2006, DC Mass) 429 F Supp 2d 385.

Service member's challenge to constitutionality of Don't Ask Don't Tell policy as regulation upon individual conduct failed; service member was unable to demonstrate that her interest in liberty was affected by government's effort to separate her from military service; because there had been no violation of her procedural due process rights, service

member could not state cause upon which relief could be granted. *Witt v United States Dep't of Air Force* (2006, WD Wash) 444 F Supp 2d 1138.

3. Standing

Plaintiffs had standing to challenge § 654(b)(1) since they all stated that they were homosexuals and thus member of allegedly disadvantaged group, statute imposes government-imposed barrier to homosexual conduct in providing for separation of servicemembers who engage, attempt to engage, or solicit homosexual acts, and Act treats homosexuals and heterosexuals differently even though they have engaged in similar acts within broad range of sexual conduct. *Able v United States* (1996, CA2 NY) 88 F3d 1280, 71 BNA FEP Cas 419, 68 CCH EPD P 44233, on remand, injunction gr (1997, ED NY) 968 F Supp 850, 71 CCH EPD P 44999, revd on other grounds (1998, CA2 NY) 155 F3d 628, 74 CCH EPD P 45501.

4. Injunction

Air Force Captain who admitted to his commanding officer that he was homosexual was not entitled to injunction preventing his discharge pending appeal since he did not have substantial likelihood of success on merits of appeal challenging constitutionality of statute, nor had he shown irreparable injury since if he prevailed on appeal he would be entitled to reinstatement with full back pay and benefits or other comparable monetary relief. *Richenberg v Perry* (1995, CA8 Neb) 73 F3d 172, 69 BNA FEP Cas 883.

Preliminary injunction will issue, in action by lesbian and gay members of United States Armed Services challenging constitutionality of new policy and regulations as to homosexuals in armed forces, enjoining United States and Secretary of Defense from investigating, discharging, or taking other adverse action against plaintiffs because they have identified themselves as homosexuals, because: (1) showing of possible violation of constitutional rights constitutes irreparable harm justifying preliminary injunction; (2) exhaustion of administrative remedies is not required when plaintiffs raise constitutional questions and when irreparable injury will occur without preliminary injunctive relief; (3) plaintiffs have established serious questions going to merits of dispute; and (4) hardship to 6 plaintiffs is evident and immediate and their free

speech rights to pursue this case will be chilled without injunctive relief, so balance of hardships tips decidedly in favor of plaintiffs. *Able v United States* (1994, ED NY) 847 F Supp 1038, 64 BNA FEP Cas 692, 64 CCH EPD P 42966.

5. Application

Servicemember who informed his commanding officer that he was homosexual failed to rebut presumption that he had propensity or intent to engage in homosexual acts, despite his testimony that he did not intend to engage in such acts, since on cross-examination he admitted to being sexually attracted to men. *Richenberg v Perry* (1996, CA8 Neb) 97 F3d 256, 68 CCH EPD P 44259, reh, en banc, den (1997, CA8) 1997 US App LEXIS 1040 and cert den (1997) 522 US 807, 118 S Ct 45, 139 L Ed 2d 12.

District court did not err in granting summary judgment with respect to military doctor's claim under Administrative Procedures Act, 5 USCS § 701 et seq., because while doctor made clear statement of intent to serve on active duty, Air Force undertook extensive investigation, conducted interview, made credibility determination, and prepared report with written findings, and concluded that doctor had informed Air Force of doctor's sexual orientation for purpose of separating. *Hensala v Dep't of the Air Force* (2003, CA9 Cal) 343 F3d 951, 2003 CDOS 8317, 2003 Daily Journal DAR 10444, 93 BNA FEP Cas 1177.

Navy servicemember's discharge from U.S. Navy on grounds that he engaged in homosexual acts must be upheld, where discharged servicemember stated to superior that he was homosexual but had never engaged in homosexual acts with other servicemen although he did frequent gay bars while off duty, which led to consensual sexual encounters, because while service members cannot be discharged solely because they are homosexuals, under Uniform Code of Military Justice (10 USCS § 654(a), (b), (f), service members may be discharged because of homosexual acts. *Philips v Perry* (1995, WD Wash) 883 F Supp 539, 66 CCH EPD P 43469, affd (1997, CA9 Wash) 106 F3d 1420, 97 CDOS 1038, 97 Daily Journal DAR 1551, 70 CCH EPD P 44721, amd on other grounds (1997, CA9 Wash) 97 CDOS 2848, 97 Daily Journal DAR 5031.

Individual, who, pursuant to military's "old policy," had been denied benefits of voluntary separation incentive and special separation benefit program (10 USCS §§ 1174a and 1175) solely on ground that individual admitted that he was homosexual, was entitled to have his eligibility reviewed under military's new policy, as codified at 10 USCS § 654; such denial of benefits raised serious equal protection questions. *Elzie v Aspin* (1995, DC Dist Col) 897 F Supp 1, 68 BNA FEP Cas 1674.

Admittedly homosexual sergeant's case is remanded with instructions that his status in Marine Corps and his eligibility for voluntary retirement program be reviewed under military's current "Don't Ask, Don't Tell" policy as codified at 10 USCS § 654, where sergeant had met all eligibility requirements for enrollment in program based on very distinguished service since 1982, but was discharged after stating publicly that he was homosexual, because new policy was enacted since discharge, and it is difficult to conceive how military's stated rationale--military morale and discipline--for discharging professed homosexuals applies to prevent homosexuals from receiving retirement benefits already earned. *Elzie v Aspin* (1995, DC Dist Col) 897 F Supp 1, 68 BNA FEP Cas 1674.

Challenge of homosexual serviceman to his separation from service under 10 USCS § 654 "Don't Ask, Don't Tell" policy is unsuccessful, where he was assigned to serve as supply officer on fast-attack nuclear submarine preparing for top secret mission, because deference towards congressional and presidential judgment in military context is great, and serviceman could not show that application of policy to his situation clearly violated his First, Fifth, or Eighth Amendment rights. *Selland v Perry* (1995, DC Md) 905 F Supp 260, 67 CCH EPD P 43897, affd without op (1996, CA4 Md) 100 F3d 950, reported in full (1996, CA4 Md) 1996 US App LEXIS 29054 and cert den (1997) 520 US 1210, 117 S Ct 1691, 137 L Ed 2d 819.

Department of Defense's "Don't Ask, Don't Tell" policy regarding homosexuals in military was constitutionally applied to servicemember, where he denied to Board of Review having engaged in any homosexual conduct with any military student or servicemember and denied engaging in homosexual conduct during performance of military duty or while on military installation, because such statements were sufficient to create presumption that he has engaged in, or has intent to engage in, homosexual conduct with nonservicemembers while off base and off duty, and such conduct may be constitutionally prohibited and provides

sufficient grounds for separation. *Watson v Perry* (1996, WD Wash) 918 F Supp 1403, *affd*, request den (1997, CA9 Cal) 124 F3d 1126, 97 CDOS 7165, 97 Daily Journal DAR 11571, 71 CCH EPD P 45000, *reh*, *en banc*, den (1998, CA9) 155 F3d 1049, 98 CDOS 7548, 98 Daily Journal DAR 10518, 74 CCH EPD P 45513 and *cert den* (1999) 525 US 1067, 119 S Ct 794, 142 L Ed 2d 657.

Servicemember's homosexual activities warranted his elimination from Army without violating any fundamental right triggering Fifth Amendment strict scrutiny on review under 10 USCS § 654; he was, however, entitled to suspension of elimination proceeding while his request for retirement was processed under Army Regulations. *Loomis v United States* (2005) 68 Fed Cl 503.

**THE SECOND ANNUAL SOLF-WARREN LECTURE IN
INTERNATIONAL AND OPERATIONAL LAW[†]**

[†] This lecture is an edited transcript of a lecture delivered on 1 April 2009 by Professor Ryan Goodman to members of the staff and faculty, distinguished guests, and officers attending the 57th Graduate Course at The Judge Advocate General's Legal Center and School, Charlottesville, Virginia. Portions of the lecture were drawn from Ryan Goodman, *The Detention of Civilians in Armed Conflict*, 103 *American Journal of International Law* 48 (2009), and appreciation is extended to the *American Journal of International Law* for permission to reprint previously published material.

The Waldemar A. Solf Chair of International Law was established at The Judge Advocate General's School, U.S. Army (TJAGSA) on 8 October 1982 in honor of Colonel (COL) Waldemar A. Solf. In August 2007, the Chair was renamed and established as the Waldemar A. Solf and Marc L. Warren Chair in International and Operational Law.

Colonel Waldemar Solf (1913–1987) was commissioned in the Field Artillery in 1941. He became a member of the Judge Advocate General's Corps in 1946. He served in increasingly important positions until his retirement twenty-two years later.

Colonel Solf's career highlights include assignments as the Senior Military Judge in Korea and at installations in the United States; Staff Judge Advocate (SJA) of both the Eighth U.S. Army/U.S. Forces Korea/United Nations Command and the U.S. Strategic Command; Chief Judicial Officer, U.S. Army Judiciary; and Chief, Military Justice Division, Office of The Judge Advocate General (OTJAG).

After two years lecturing with American University, COL Solf rejoined the Corps in 1970 as a civilian employee. Over the next ten years, he served as Chief of the International Law Team in the International Affairs Division, OTJAG, and later as chief of that division. During this period, he served as a U.S. delegate to the International Committee of the Red Cross (ICRC) Conference of Government Experts on Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts. He also served as Chairman of the U.S. delegation to the ICRC Meeting of Experts on Signaling and Identification Systems for Medical Transports by Land and Sea.

He was a representative of the United States to all four of the diplomatic conferences that prepared the 1977 Protocols Additional to the 1949 Geneva Conventions. After his successful efforts in completing the Protocol negotiations, he returned to Washington and was appointed the Special Assistant to The Judge Advocate General for Law of War Matters. Having been instrumental in promoting law of war programs throughout the Department of Defense, COL Solf again retired in August 1979.

In addition to teaching at American University, COL Solf wrote numerous scholarly articles. He also served as a director of several international law societies, and was active in the International Law Section of the American Bar Association and the Federal Bar Association.

Colonel (Ret.) Marc Warren served in the U.S. Army Judge Advocate General's Corps as the Special Assistant to The Judge Advocate General and as the Staff Judge Advocate (senior attorney) for Combined Joint Task Force 7/Multi-National Forces in Iraq, V Corps in Iraq and Germany, and the 101st Airborne Division (Air Assault). He was the Legal Advisor for the world-wide activities of the Joint Special Operations Command, Regimental Judge Advocate for the 11th Armored Cavalry Regiment, and served in numerous other assignments as a Judge Advocate in the United States, Germany, Grenada, Bosnia, Kuwait, and Iraq. His awards and decorations include the Distinguished Service Medal, Defense Superior Service Medal, the Legion of Merit, and

PROFESSOR RYAN GOODMAN*

Thank you very much for that introduction. I want to begin by saying how special an honor and pleasure it is for me to be here with you and engage you on this topic and discussion. I've thought very specifically about the ways in which it's an honor and pleasure for me. First, I regard you as an exceptional audience. I'm deeply respectful and grateful for your service to the country, and I'm also keenly aware that you have been thinking about these topics and will be thinking about these topics a lot, probably much more than me and especially collectively by magnitudes more than me. So I'm very much looking forward to our conversation after the presentation. It's also an honor and a privilege for me to be here given that this distinguished lecture series is in the name of Colonels Solf and Warren, and it's also humbling given the extraordinary individuals who have been invited to speak on prior occasions of this

the Bronze Star Medal. He has earned the master parachutist, pathfinder, and air assault badges.

Colonel Warren was appointed as the FAA's Deputy Chief Counsel for Operations in November 2007. He assists the Chief Counsel in overseeing all aspects of the FAA's legal activities with special focus on nationwide enforcement, airports and environmental, personnel and labor law, and Regional and Center Counsel office activities.

Colonel Warren received the B.A. and J.D. degrees, with honors, from the University of Florida; an LL.M. degree from the Judge Advocate General's School; and a Master of Strategic Studies degree from the U.S. Army War College. He is a member of the Florida Bar.

* Ryan Goodman is the Rita E. Hauser Professor of Human Rights and Humanitarian Law, and Director of the Human Rights Program at Harvard Law School. Professor Goodman received his J.D. from Yale Law School, where he served as an articles editor of the Yale Law Journal. He received a Ph.D. in Sociology from Yale University, and he received a B.A. from the University of Texas at Austin. Professor Goodman clerked for Judge Stephen Reinhardt of the U.S. Court of Appeals for the Ninth Circuit. He has worked at the U.S. Department of State, the International Criminal Tribunal for the former Yugoslavia, and various nongovernmental organizations in India, South Africa, Switzerland, Thailand, and the United States.

Professor Goodman's publications have appeared in the *American Journal of International Law*, the *Duke Law Journal*, the *Harvard Law Review*, the *Stanford Law Review*, and the *Yale Law Journal*. His publications also include the following books: *International Human Rights in Context* (Oxford University Press, 3d ed., 2007) (with Henry Steiner & Philip Alston); *Socializing States: Promoting Human Rights through International Law* (Oxford University Press, forthcoming) (with Derek Jinks); *International Humanitarian Law* (Oxford University Press, forthcoming) (with Derek Jinks & Michael Schmitt); and *Understanding Social Action, Promoting Human Rights* (Oxford University Press, forthcoming) (with Derek Jinks & Andrew K. Woods).

Professor Goodman is a member of the Board of Editors of the *American Journal of International Law*. His research interests include public international law, international human rights law, and international relations.

distinguished lecture series. I also want to express my gratitude for the hospitality that's been shown to me by the faculty, staff, and students when I had to postpone this lecture due to an unforeseen family illness. When I received the re-invitation to come, at a later occasion, there was a paranoid part of me that thought it might be a joke given that we had scheduled this for April Fool's Day. So it's a relief to actually see that the auditorium has people in it besides myself.

The discussion that I want to engage in with you today is the question of the detention of civilians in the armed conflict with al Qaeda, or more particularly, the question concerning *which* civilians can be detained in the armed conflict with al Qaeda. It's obviously an extraordinarily timely topic, more timely than I had even imagined when the date for this event was scheduled. What's taken place, just to make sure that we're all on the same page, is that the Supreme Court has expressed its interest in deciding the matter, if it remains controverted, by having granted cert in the *Al-Marri*¹ case. The Court subsequently dismissed the case as moot, but the Justices are presumably keeping a watchful eye on the developments that take place. Also since January there have been congressional bills introduced that would redefine the application of detention authority with respect to enemy combatants whether or not that term is used, and the administration is now engaged in a multiagency review of the question. Just a couple of weeks ago, the Department of Justice submitted a memo in the *In re Guantanamo Detention Litigation* staking out its preliminary position on this topic. I will talk to you about my paper on which this presentation is based,² and I will also incorporate these more recent events.

I have organized the presentation in three parts. The first part outlines the long-standing law of armed conflict framework. In other words, I want to examine the regime that constitutes the legal background against which post-9/11 policies, practices, and representations were made by the Government, by civil society actors, and others. The second part of the presentation describes and identifies misunderstandings or misconceptions of that legal framework that have occurred over the last eight years, on the part of the Executive Branch, members of Congress, some federal judges, and litigators. So in some ways no group escapes that kind of a challenge or critique. The third

¹ *Al-Marri v. Pucciarelli*, 534 F.3d 213 *passim* (4th Cir. 2008) (en banc).

² Ryan Goodman, *The Detention of Civilians in Armed Conflict* 103 AM. J. INT'L L. 48 (2009).

part of the lecture describes the consequences or implications of those misunderstandings.

First, let's look at the structure of the existing framework that long predated 9/11. Before I turn to the table, I should say a few words about the material field of application with respect to noninternational armed conflicts. I accept and take as granted that we are currently in an armed conflict with al Qaeda which is governed at least by Common Article 3,³ all three branches of the U.S. Government have agreed to that proposition, and we can open it up to discussion if you'd like to, but I'm taking it as an accepted premise for the purpose of this initial presentation.

I should also note that I naturally understand that status-based categories, like prisoners of war, do not apply in noninternational armed conflicts, and therefore I'll generally refer to classes of actions and classes of individuals, such as civilians or direct participation in armed conflict, which have referents in conventional sources like Common Article 3⁴ and Additional Protocol II⁵ to the Geneva Conventions, but, as you can tell from the table, I will refer to part of the legal regime that applies to international armed conflict as well. And I want to give you three reasons why I think it's relevant that we consider the legal regime applicable in international armed conflict before, then transposing it or applying it to the noninternational armed conflict with al Qaeda. This is especially important because the Department of Justice memo that was submitted in recent litigation in fact states that such an analytic move is a predicate for the position of the administration.

Three reasons justify that application. The first is a reactive reason; simply put, many commentators and practitioners have applied the law of international armed conflict to the conflict with al Qaeda by analogy. It's a prevalent practice that's used, for example, in debates about whether or not we can hold fighters until the cessation of hostilities and with or without access to an attorney. The analog or the referent in those discussions is often international armed conflict. And if that's a prevalent mode of discourse or argument, then we at least need to

³ Geneva Convention Relative to the Treatment of Prisoners of War art. 3, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter GC III].

⁴ *Id.*

⁵ Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), June 8, 1977, 1125 U.N.T.S. 609 [hereinafter AP II].

understand better the referent, which is the law of international armed conflict, to evaluate those kinds of claims.

A second reason is an affirmative one. On my view, it's valid to use the law of international armed conflict as an analogy. In fact, if we have to think of an analogy, it's the closest fit or closest approximation—especially the Fourth Geneva Convention⁶—for questions of who may be detained and what types of activities on the part of civilians are subject to detention. That is, the rules contained in the Civilians Convention, are the closest analog that we have and therefore the best reference point for trying to approximate what the law of armed conflict should look like or will look like when it applies in a noninternational scenario like the conflict with al Qaeda.

The third reason is the strongest, and it's an affirmative argument not just by way of analogy. The argument here is that the law in international armed conflict establishes an outer boundary of permissive action. The idea is fairly simple, which is that the law of armed conflict uniformly involves more exacting, more restrictive obligations on parties in international armed conflict than in noninternational armed conflict. We could even state this point as a maxim: if states have authority to engage in particular practices in an international armed conflict, they *a fortiori* possess the authority to undertake the same practices in noninternational armed conflict, or simply put, whatever is permitted in international armed conflict is permitted in noninternational armed conflict. Therefore, if the law of armed conflict permits a state to detain civilians in international armed conflict, the law of armed conflict surely permits states to detain civilians in a noninternational armed conflict. The same logic does not apply to prohibitions or proscriptive rules: it does not follow that if the law of armed conflict forbids states from engaging in a practice in international armed conflict that the law would also forbid states from engaging in that practice in noninternational armed conflict. Nevertheless, I think we'll see in our discussion that the permissive rules are sufficient to answer many of our questions, and the remaining open questions concerning what else is forbidden will be answered by other ordinary sources of international legal authority that have addressed the question whether a party can preventively detain civilians who pose no security threat. So those remaining questions, in the end, will be fairly easy to answer.

⁶ Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter GC IV].

The table that I've created tries to make sense of the existing legal framework.

Actions Permitted by the Law of Armed Conflict

		COERCIVE MEASURES		
		I. Targeting	II. Military Trial	III. Detention
SUBJECTS	A. Members of regular armed forces and irregular forces that meet Geneva Convention III or Additional Protocol I criteria	(1) YES	(2) YES	(3) YES
	B. DPH: Direct participants in hostilities (“unlawful combatants”)	(4) YES	(5) YES	(6) YES
	C. IPH: Indirect participants in hostilities (security threats)	(7) NO	(8) NO?	(9) YES
	D. NPH: Nonparticipants in hostilities (“innocent civilians”)	(10) NO	(11) NO?	(12) NO

The substantive rules reflected in the table are meant to reflect the structure of the law of armed conflict with respect to the detention of civilians, in particular, as well as interactions or relationships with other elements of the law of armed conflict regime. In that respect it's useful

to distinguish three types of coercive measures. The table thus distinguishes targeting, military trial, and detention across four different groups of individuals. Group A includes members of regular armed forces and irregular forces that meet either Geneva Convention III⁷ or Additional Protocol I⁸ criteria, with the obvious caveat that the U.S. Government has not ratified Protocol I⁹ and considers many of its provisions, especially these, not reflective of customary international law. But with that caveat, we can still usefully proceed because the U.S. Government would just place some of those individuals in Group “B”; and as you can tell from the rows for Groups “B” and “A,” it actually makes no difference. The Group “B” category includes direct participants in hostilities, otherwise referred to as unlawful combatants with scare quotes, or unprivileged belligerents. These are civilians who directly participate in hostilities without the lawful prerogative to do so. Group “C” is what I’m calling indirect participants in hostilities, otherwise known as imperative security threats, that is, individuals who would be classified under the Fourth Convention as a threat to the state and may be detained as such.¹⁰ And I’ll say a lot more, not just a little more, but a lot more about who might fit within that category. The final group of actors is nonparticipants in hostilities, what some authorities refer to as “innocent civilians;” that caption is generally a lay term which nevertheless captures the idea that these individuals have no meaningful relationship to or contribution to the war effort or to hostilities.

The big point of the table is to demonstrate the relationships between the cells, not necessarily the content of the cells. I understand, however, that I can’t escape delving into the content, especially because some of the content is controversial. So let me say just a few words about what is contained in direct participation, and cell number four is the flagship in terms of what most of the debate has been about in the last several years with respect to the International Committee of the Red Cross’s (ICRC) study on direct participation. That ongoing study focuses primarily on direct participants for the purpose of targeting, not for the other reasons. That said, let me provide a preliminary definition of what we might mean by “direct participation.” It is generally defined to have a geographic

⁷ Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter GC III].

⁸ Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 U.N.T.S. 3, 37–38 [hereinafter AP I].

⁹ *Id.*

¹⁰ GC IV, *supra* note 6, arts. 5, 27, 41–43 & 78.

and temporal proximity to the damage inflicted on the enemy. To take from the ICRC's Commentaries on the Additional Protocols, "direct participation in hostilities implies a direct causal relationship between the activity engaged in and the harm done to the enemy at the time and place where the activity takes place," and it entails, "a sufficient causal relationship between the act of participation and its immediate consequences." There are persistent definitional squabbles about the category. Many of those definitional squabbles, however, demonstrate how well-settled a core part of the category actually is. It's always a curiosity to me that the example usually given to show the lines of debate on the definition involves a civilian who drives a truck full of ammunition to the front lines, and the question posed is whether that individual is a direct participant. To me, that demonstrates how much we must know because that scenario is so close to direct participation. The fact that scenario would be controversial demonstrates in a sense how much is noncontroversial. Indeed, important elements are fairly well-settled. Just look to the POW Convention, Article 4(A)(4):¹¹ persons accompanying the armed forces are clearly not direct participants. They, in fact, don't have the right to participate directly in hostilities; so we do know that a category of actors engaged in logistical support to armed forces, even in the zone of active military operations, fall below the threshold. Persons accompanying armed forces, such as, "supply contractors [and] members of labor units or of services responsible for the welfare of the armed forces," are noncombatants by the strict terms of the treaties. Nils Meltzer has recently written—and this will be important when we evaluate the Department of Justice's memo—in the case of noninternational armed conflicts with irregularly constituted armed groups that "religious leaders . . . financial contributors, informants, collaborators and other service providers without fighting functions [who] may support or belong to an opposition movement or an insurgency as a whole can hardly be regarded as members of its 'armed forces' in the functional sense underlying [the law of armed conflict]." That's fairly controversial in a way. I don't want to represent that statement as though it is black letter law, but it gives you a sense of where some of that debate has transpired without a necessary connection to the armed conflict with al Qaeda.

With regard to targeting, the table demonstrates, for example, the fundamental principle of distinction. The major difference under Column I for targeting is between Groups A and B and Groups C and D,

¹¹ GC III, *supra* note 7.

so the dividing line between B and C constitutes the distinction between those who directly participate or not. If a civilian directly participates, they lose their immunity from direct attack. In contrast, for detention there's a very different line that is drawn, which will be the most important line for our discussion. The line that's drawn for detention, so Column III, is between C and D. In other words, A, B, and C are all subject to lawful detention, direct participants and indirect participants alike. As a result, I have a burden to carry out by saying a little more about what actors or actions fall under Category D as opposed to Category C for the purpose of detention.

So, who are nonparticipants versus indirect participants in hostilities? A fundamental principle of the law of armed conflict is that it forbids the detention of individuals solely because they are nationals or part of the general population of the enemy power. Their political sympathy or political affiliation is not sufficient to indicate indirect participation in hostilities. Instead, a specific determination must be made that each civilian who is detained poses a threat to the security of the state. So we find in Category C, the security threats to the state, otherwise located in Articles 5, 27, 41 through 43, and 78 of the Civilians Convention.¹² The ICRC Commentary and an excellent article in the *Military Law Review* by Colonel Robert Gehring clearly demonstrate that the category of security detainees is broader than the category of direct participants in hostilities.¹³ And also the Third Convention is fairly clear about it. That is, the POW Convention, not just the Civilians Convention, specifically contemplates the detention of individuals who are not direct participants in hostilities. Persons, sometimes referred to as civilians, who accompany the armed forces, may be detained without a finding that the individuals have directly participated in hostilities. The definition of indirect participants in hostilities does not imply a direct causal relationship or geographical proximity between the individual's activity and the damage inflicted on the enemy, which is in contrast to direct participation in hostilities. Indeed, the activity need not occur on a battlefield. For example, the ICRC's Commentary states, "Subversive activity carried on inside the territory of a party to the conflict or actions which are of direct assistance to an enemy power"¹⁴ count as indirect

¹² GC IV, *supra* note 6.

¹³ Captain Robert W. Gehring, *Legal Rules Affecting Military Use of the Seabed*, 54 MIL. L. REV. 168 (1971).

¹⁴ ICRC, COMMENTARY: IV GENEVA CONVENTION RELATIVE TO THE PROTECTION OF CIVILIAN PERSONS IN TIME OF WAR, art. 42, at 258 (Jean S. Pictet gen. ed., 1958).

participation, or as a security threat. Michael Bothe and his colleagues, in a well-regarded treatise on noninternational armed conflict, refer to a category of “civilians who support the armed forces (or armed groups) by supplying labour, transporting supplies, serving as messengers or disseminating propaganda,” who are not direct participants according to the treatise, “but they remain amenable to domestic legislation against giving aid and comfort to domestic enemies.”¹⁵ Hence many of those functions that are currently carried out, for example, on behalf of the U.S. Government by private military contractors would constitute indirect participation, not direct participation, subject to detention though not subject to lethal force or direct attack.

One important note: I’ve just defined the category but I haven’t defined it specifically within the context of detention. It’s important to note that in detention not only do we need to define what individuals or activities fall within that category, but there’s a separate element that we might address in our discussion following my remarks, which is that the detention must be absolutely necessary for the security of the state. Thus, there’s an independent test that might come into play, depending on what particular issue or coercive measure is under consideration.

A second note, before moving on, is that states are given very wide latitude in defining a threat to their security. The ICRC Commentaries make such an acknowledgement explicit. At the same time, however, Richard Baxter, in a leading article, demonstrated that abuse of such discretion constitutes a war crime,¹⁶ and Additional Protocol I, for example, shows that abuse of such discretion constitutes a grave breach, which places important boundaries on decisions made in the detention context.

The last point to make is that I think everything I’ve said so far is relatively noncontroversial. It’s fairly well-settled and understood. In fact, I’m worried that I’m boring you! What’s not well-settled are cells number 8 and 11. So, I should say a few words about them, even though they’re not the main focus of my remarks. It’s important to understand the entirety of the regime including the legality of military trials. I’m not

¹⁵ MICHAEL BOTHE, KARL JOSEF PARTSCH & WALDEMAR A. SOLF, *NEW RULES FOR VICTIMS OF ARMED CONFLICTS: COMMENTARY ON THE TWO 1977 PROTOCOLS ADDITIONAL TO THE GENEVA CONVENTIONS OF 1949*, at 672 (1982).

¹⁶ Richard R. Baxter, *The Duty of Obedience to the Belligerent Occupant*, 1950 BRIT. Y.B. INT’L L. 235.

fully certain whether a party to a conflict can conduct a military trial for a civilian who is not a direct participant in hostilities. If we referred to Categories A and B as “combatants,” whether lawful combatants or unlawful combatants, and Category C and D, as “civilians” who are not directly participating in hostilities, there’s an open question whether the law of armed conflict forbids military trials of those civilians. Many have referred to the Civil War case by the Supreme Court in *Ex parte Milligan* as standing for the proposition, at least read through contemporary eyes, that the law of war precludes military trials for civilians.¹⁷ Gary Solis submitted a declaration in the *Boumediene*¹⁸ case that also contends that a party cannot hold military trials for civilians.¹⁹ It is unclear what the textual source for that proposition might be. The Geneva Conventions are arguably silent on the matter as to whether a military trial can be held for civilians and, in fact, the Fourth Convention in Article 66 does permit some military trials for civilians in an occupied setting.²⁰ That said, there are now a plethora of sources in the international human rights realm that reach the conclusion that military trials are permitted only when civilian courts are closed or unavailable in circumstances such as occupation or martial law, such that resorting to the military system is essentially “unavoidable.”

Against that background legal regime, let’s now consider the category mistakes that have violated the existing framework. I want to discuss three different types of category mistakes. As you’ll see from the slide presentation, I’ll elaborate the content of each of these: first, actor conflation; second, actor disaggregation; and, third, power conflation.²¹

As a caveat, I do agree that it’s perfectly reasonable and appropriate to advocate for changes in the law, to adopt a normative position, and to suggest that the framework shouldn’t be applicable to the present conflict, but that’s a very different kind of an argument than the arguments that I’m going to present on the screen. The arguments I’m going to present are made by commentators and practitioners who are not involved in such normative projects; instead, they are purportedly working with the fixed foundation of existing rules, that is, referring to the existing rules but conflating or disaggregating domains of actors and

¹⁷ 71 U.S. (4 Wall.) 2 (1866).

¹⁸ Gary D. Solis, Declaration, *Boumediene v. Bush*, 583 F.Supp.2d 133 (D.D.C. 2008) (Civ. No. 04-1166 (RJL)), available at 2008 WL 5260271.

¹⁹ *Id.* para. 6.f.

²⁰ GC IV, *supra* note 6, art. 66.

²¹ See Appendix A.

coercive powers without sufficient explanation or recognition of the novelty of that venture.

The first type of category mistake is actor conflation. This category mistake has been made primarily by proponents of current U.S. detention policy. As the previous slide showed, a fundamental category mistake involves grouping different actors under a heading that correctly applies only to some of them. For example, only Groups A and B in the table included combatants. The U.S. Government, however, has officially taken the position that the definition of combatants also includes members of Group C, indirect participants in hostilities. So the position I'm maintaining is a fairly clear one. Lawful combatants and direct participants in hostilities can be called combatants. But individuals who provide logistical support and the like, civilians who accompany the armed forces, are not combatants; they're civilians who are security threats. Now this might be immaterial or semantic at one level because all of those individuals can be detained. At the end of my talk, however, when I discuss the implications, I will explain the significant consequences from reorganizing the categories, especially without admitting or recognizing that one is engaging in such an innovative venture.

The following slide presents, in chronological order, various representations of the law on the part of the U.S. Government and U.S. federal judges.²² The Department of Defense, in a Fact Sheet issued in February 2004, employed a definition of enemy combatants that is perfectly consistent with the existing standard for direct participation in hostilities. The idea here, as you can see from the slide,²³ is that the individual must be part of or supporting forces hostile to the United States, and that individual must also be engaged in an armed conflict against the United States. That is, individuals themselves must be personally engaged in the armed conflict. It is insufficient, according to that definition, if an individual only supports others who are engaged in the armed conflict, as an indirect participant might do. In short, the Government has to make a finding that is equivalent to or consistent with

²² See Appendix B.

²³ U.S. Dep't of Def., Fact Sheet: Guantanamo Detainees 5 (Feb. 13, 2004), available at www.defenselink.mil/news/Feb2004/d20040220det.pdf ("At the time of capture and based on available information, combatant and field commanders determine whether a captured individual was part of or supporting forces hostile to the United States or coalition partners, and engaged in an armed conflict against the United States. Such persons are enemy combatants.").

the direct participation standard. The U.S. Government, in its brief submitted to the Supreme Court in *Hamdi*,²⁴ referred to that Fact Sheet, and then the Supreme Court, in a plurality opinion, adopted essentially the same definition with a citation to the Government's brief.²⁵ In the plurality's construction, a great deal might turn on the word "who." Indeed, within weeks after *Hamdi*, the Combatant Status Review Tribunals order was issued, and the word "who" changed to "that," and under that system, the definition of a combatant is "an individual who was part of or supporting Taliban or al Qaeda forces or associated forces *that* are engaged in hostilities."²⁶ As a consequence, the Government need not make a finding that the individual directly engaged in fighting; the Government needs to prove only that the individual supported Taliban or al Qaeda forces and those forces directly participated or engaged in hostilities. As the next section of the slide shows, Congress essentially ratified, or endorsed, that position since the Military Commissions Act (MCA)²⁷ adopts a very similar definitional structure. The MCA also refers to an individual "who has purposefully and materially supported hostilities," which could encompass indirect participants in hostilities.

Finally, let me end with an example of one of the most notorious interpretations of what such standards might encompass. I assume that many of you are familiar with it. In the *In re Guantanamo Litigation* before District Court Judge Joyce Green, the Government attorney answered a hypothetical question in which Judge Green asked whether the CSRT definition of an enemy combatant could apply to "a little old lady in Switzerland who writes checks to what she thinks is a charity that helps orphans in Afghanistan but [what] really is a front to finance al-Qaeda activities." The attorney for the Government responded that the unknowing, little old lady in Switzerland would count. Now, I do not want to pin my argument on that extreme claim, but it does show you, at least in some nontrivial sense, how a slippery slope might work.

²⁴ Brief for Respondents, at 3, *Hamdi v. Rumsfeld*, 542 U.S. 507 (4th Cir. 2004) (No. 03-6696).

²⁵ *Hamdi v. Rumsfeld*, 542 U.S. 507, 516 (2004) (quoting Brief for the Respondents at 3, *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004) (No. 03-6696), available at 2004 WL 724020 ("an individual who . . . was 'part of or supporting forces hostile to the United States or coalition partners' in Afghanistan and who 'engaged in an armed conflict against the United States' there.") (emphasis added) (internal quotation marks omitted)).

²⁶ Deputy Secretary of Defense Paul Wolfowitz, Memorandum to the Secretary of the Navy 1 (July 7, 2004) (emphasis added), available at www.defenselink.mil/news/Jul2004/d20040707review.pdf.

²⁷ Pub. L. No. 109-366, 120 Stat. 2600 (2006).

Roman numeral five on the slide contains a quotation from the DoJ's memo issued in March 2009.²⁸ The memo does not define enemy combatant, which makes this a very different proposition. Everything else up to this point in my presentation involved a definition of enemy combatant, which potentially included slippage in conflating indirect participants with direct participants. Here, the Government is not taking a position with respect to the definition of enemy combatants, but the new position is largely reflective of the Combatant Status Review Tribunal's definition.²⁹ Apparently many, if not all, of the very same individuals can be detained, and, under the framework that I articulated earlier, that result is permitted by the law of armed conflict because a state can detain direct participants and indirect participants. The question of nomenclature is eliminated; but, as you can see on the slide, a significant distinction involves the terms "substantially supported." That's different from the unqualified term "supported" under the Combatant Status Review Tribunal. It is also interesting to compare the Military Commissions Act, because the MCA contains "purposefully and materially supported." Thus the delta between those two standards—the DoJ memo and the MCA—might be very small.

Let me make a couple preliminary remarks about the new definition. In my view, if we are to work within the existing international legal framework, it might be better to maintain an explicit reference to enemy combatants and then add an express reference to civilians who indirectly participate in hostilities. The DoJ position makes a valuable advance, but it also raises concerns. First, it's underspecified. We don't know what it means to be a member in an armed group, and that's why I used the Nils Meltzer quote from before. According to his study, "religious leaders . . . financial contributors, informants, collaborators and other service providers without fighting function [who] may support or belong to an opposition movement or an insurgency as a whole can hardly be regarded as members of its 'armed forces.'" So it's an open question what membership in the armed forces entails. Much of what one cares most about might turn on that very question.

The next concern with the DoJ memo is the question of mere membership. Is mere membership in a group sufficient? A very insightful analysis can be found in a recent decision by Israel's High

²⁸ See Appendix B.

²⁹ Respondents Memorandum, *In re Guantanamo Litigation* (D.D.C. Mar. 13, 2009) (Misc. No. 08-442), available at <http://www.usdoj.gov/opa/documents/memo-re-det-auth.pdf>.

Court. The Israeli Court, dealing with a very similar statute and a similar set of concerns, concluded that mere membership in the armed forces or terrorist organization is not enough.³⁰ That proposition, however, is not necessarily endorsed by the reasoning in the DoJ memo.

The last concern about the DoJ memo involves the work being done by the terms “substantially support.” There’s one statement in the memo which seems to suggest that the new definition might not escape all the concerns that we would otherwise have about the Combatant Status Review Tribunal definition and the Military Commissions Act definition. The concern is triggered if “substantially supports” performs a function of assimilation, whereby an individual who engages in substantial support is considered a member of the fighting forces. That equation could spell trouble because it would mean the same conflation of Category C, indirect participants in hostilities, with Category B. The troubling sentence in the memo is “Under a functional analysis, individuals who provide substantial support to al-Qaeda forces in other parts of the world may properly be deemed part of al-Qaeda itself.”³¹

Turning to another pattern that has occurred over the past several years, I also want to discuss actor disaggregation. The concern here is a second type of category mistake, which involves the failure to properly recognize that certain distinct categories of individuals are all lawfully subject to the same coercive measure. For example, it’s improper to suggest that a state can legally target Group A, lawful combatants, but not legally target Group B, direct participants. Similarly, litigators who have represented the interests of detainees in Guantanamo and elsewhere criticized the Government for an expansive definition of combatant that includes civilians who do not meet the direct participation standard; however, those opponents do not acknowledge that the law of armed conflict permits the very same individuals to be detained, regardless of the nomenclature or the name that one assigns the individuals. Some opponents have even taken a stronger position, contending that only combatants can be detained and that Category C cannot be detained, which, in my view, flies in the face of the existing framework. Let’s now consider *Al-Marri*, the case in which the Supreme Court granted certiorari but then subsequently vacated because the individual was transferred to the civilian system for criminal prosecution. On the slide

³⁰ A. v. State of Israel, Cr. App. 6659/06 (S. Ct. Israel, June 11, 2008), available at http://e1yon1.court.gov.il/files_eng/06/590/066/n04/06066590.n04.pdf.

³¹ *Id.*

is an excerpt from the opinion which is otherwise termed “the plurality opinion” in the Court of Appeals decision. Three other judges joined this opinion. Ultimately, their view on this legal issue did not affect the holding. Yet it is technically a plurality opinion with respect to the traditional law of war understanding of who may be detained. The other judges on the panel didn’t agree on that issue. Four judges took the position that under the long-standing law of armed conflict, civilians cannot be detained. The quote on the slide gives you one example of it: Judge Motz states that “‘civilian’ is a term of art in the law of war, not signifying an innocent person, but rather someone in a certain legal category who is not subject to military seizure or detention. So, too, a ‘combatant’ is by no means always a wrongdoer, but rather a member of a different ‘legal category’ who is subject to military seizure and detention. . . . Nations in international conflicts can summarily remove the adversary’s ‘combatants,’ i.e., the ‘enemy combatants,’ from the battlefield and detain them for the duration of such conflicts, but no such provision is made for ‘civilians.’” The opinion never refers to the articles of the Fourth Convention that I’ve discussed. The opinion never refers to Article 4(A)(4) of the POW Convention in this regard either.³²

One of the concerns you might think about is why did the judges reach that opinion? On the screen are various quotes from legal briefs filed by litigators on behalf of detainees. Not all the briefs are like this, however. I’ve picked only the briefs that make the category mistake of representing to the judges that civilians cannot be detained in an armed conflict if they’re not direct participants. So the bolded language (on the slide) gives you a sense of these portrayals of the law. The appellant in *Al-Marri* said, by contrast, “[A]rresting civilians in their homes inside the United States, far from any active battlefield, and detaining them in military custody is not a fundamental incident of war.” The petition for cert in *Al-Marri* said, “Hewing to the laws of war, this Court’s decisions consistently construe military detention power in light of this law-of-war principle, allowing military jurisdiction to be exercised only over members of an enemy nation’s military, militia, or other armed forces, and those who fight alongside them on a battlefield, such as Al Qaeda fighters in the war of Afghanistan.” Petitioners in *Boumediene* said, “*Hamdi* emphasizes that military detention is justified only ‘to prevent a combatant’s return to the battlefield.’ Civilians who do not directly participate were never on the ‘battlefield’ in the first place, and therefore there is no justification for treating them as ‘combatants who might

³² GC III, *supra* note 7.

return.’ Of course civilians may be punished for activity short of direct participation in hostilities, even though they cannot be targeted with military force or subjected to military detention.” And then the last one, as well, is, as you can tell from the slide, very similar.

The last category mistake I want to discuss is power conflation. Here both proponents and opponents have made the mistake of conflating the power to detain with the power to prosecute. It’s important to note before mentioning instances of this conflation—and you can see a couple of them on the next slide—that under the existing framework of the law of armed conflict, detention is generally considered a less restrictive means than military trial. So, military trial is the greater power, and detention is the lesser power. Interestingly, the same principle indeed applies in international human rights law as well. The Covenant on Civil and Political Rights is very similar to the Geneva Conventions whereby there are several procedural requirements that apply to trials that are considerably more stringent than the procedures that apply to detention. The logic underlying this system is that a trial is thought to be a much more severe measure, and detention is considered a less severe, less restrictive measure.

Proponents of U.S. detention policy have tied the power to conduct military trials with the power to detain. Consider the decision in *Hamdi*. The plurality opinion references the *Milligan* Civil War case in stating that if combatants could be tried by a military court, then they could also be detained,³³ and that might be a fair, logical argument—if a state possesses the greater power, the state certainly has the lesser power—but it demonstrates that the reverse doesn’t work. In his dissent, Justice Scalia interestingly seems to recognize that there’s a problem in transposing the rules for military trial into detention, yet he still makes that very transposition. As you can see in the slide, he states that “*Milligan* is not exactly this case, of course, since the petitioner was threatened with death, not merely imprisonment. But the reasoning and conclusion of *Milligan* logically cover the present case. The Government justifies imprisonment of Hamdi on principles of the law of war and admits that, absent the war, it would have no such authority. But if the law of war cannot be applied to citizens where courts are open, then Hamdi’s imprisonment without criminal trial is no less unlawful than *Milligan*’s trial by military tribunal.”³⁴ Judge Motz made the same

³³ *Hamdi*, 542 U.S. at 522.

³⁴ *Id.* at 567–68 (Scalia, J., dissenting).

error in *Al-Marri*, claiming that if a state cannot try a civilian before a military court, then a state cannot militarily detain the individual.³⁵ That reasoning doesn't work, because it would mean that the lesser power includes the greater power, in a certain sense. It is also important to note that even if this reasoning were sustainable, it would only deny military detention. It wouldn't deny detention by civilian authorities.

As a final part of my presentation, let me discuss the impact of these misclassifications or miscategorizations. The first impact is a general consequence of ambiguity in the legal regime. And here, I want to momentarily wear my other hat. The other hat that I sometimes wear is that of an interdisciplinary scholar. I study, as an empirical matter, what drives state behavior, what motivates actors to comply or violate international law. It's fair to say that there are two schools of thought: one is normative and emphasizes how actors follow a logic of normative appropriateness, and the other is instrumental and emphasizes how rational actors following a logic of consequences. Both schools of thought would be deeply troubled by the introduction of ambiguity into international law. The argument for the normative model of behavior is that, according to widely accepted theories, clarity in the law is essential to its legitimacy, and if legitimacy erodes, then compliance with law erodes. The rational actor model, which is based more on systems of incentives, also requires clarity in the law. In that case, the introduction of ambiguity undermines the clarity of the law that is required for individuals to know whether or not their actions are cooperative or uncooperative, compliant or noncompliant. And, as the slide suggests, the introduction of significant ambiguity also raises a fundamental question of fairness. Should we apply unclear standards to operators, when those standards could result in criminal penalties or social sanctions, or damage to a person's reputation? This question of fundamental fairness applies to arguments on all sides—some of the arguments that have been made by proponents, some of the arguments that have been made by opponents.

Let me next turn attention to the consequences of some of the opponents' positions, that is, opponents of U.S. detention policies since 9/11. As the slide suggests, one consequence is that these arguments misdirect legal and policy efforts. A false impression has been created that a solid legal edifice underpins the claim that civilians cannot be detained in armed conflict where, in fact, that legal edifice doesn't exist.

³⁵ *Al-Marri v. Pucciarelli*, 534 F.3d 213, 230–31, 237 n.19 (4th Cir. 2008) (en banc).

Accordingly, insufficient attention has been paid to alternative legal and policy grounds for developing principled constraints on detentions. More viable approaches may be found through the political process and policy changes, not litigation; or directly in constitutional law, not directly in the law of armed conflict.

Let me elaborate briefly. First, the law of armed conflict permits the detention of individuals who are indirect participants in hostilities. Whether, as a policy matter, it's wise to go as far as the law allows is a separate and important question. And that's where a policy debate should take place. Should U.S. policy extend to the outer boundary of what international law permits? Will that strategy win more hearts and minds? Will it damage our public and social institutions? Second, if one pursues a legal claim against current detention practices, consider underexploited U.S. domestic law options. For example, the U.S. Constitution arguably distinguishes between the exercise of military control over civilians versus combatants. And, in that case, the definition of civilians versus combatants could be found in the law of armed conflict. But the fundamental question concerns constitutional and domestic law. Thus a very strong argument could be made that if Congress truly wants to detain civilians who are indirect participants in hostilities, it has to say so plainly on the face of the statute; and Congress has not done that so far. But that would be a domestic legal question. And I'm no expert in that arena.

The second consequence of opponents' positions concerns coercive powers over enemy private contractors. A logical consequence of their arguments is that private military contractors whose activities constitute only indirect participation in hostilities would not be detainable. Yet such a result seems inconsistent with the opponents' own views and values. Many of those opponents understandably are concerned about the potential security threats that military contractors pose on the battlefield, but their argument undermines the basis for the detention of such actors. It would also be vexing to military commanders, U.S. military commanders included, who might face the need to detain enemy private contractors during hostilities.

The third consequence is an erosion of prohibitions on the use of child soldiers. These same opponents of detention are generally sympathetic to efforts to strengthen the regime that prohibits children from directly participating hostilities. But, by narrowly defining what it

means to directly participate in hostilities, their argument creates a loophole in the child soldiers regime.

A fourth consequence is a potential expansion of the class of actions that are subject to lethal force. There are two dynamics here. One is a self-fulfilling effect. In legal briefs that have been filed before federal courts, some have adopted a two-pronged argument: namely, if the court were to accept that civilians who are indirect participants in hostilities could be detained, the court must also accept that those individuals would be lawful targets. That argument is based on either a claim that the powers to engage in such coercive measures, detention and targeting, are coextensive with one another, or a claim that the law on detention is derivative of the law on targeting. In other words, the only people who may be detained are those who can be targeted. Both of those claims are incorrect. But if the opponents' argument loses on the first prong—that is, if a court concludes that indirect participants can be detained—then the self-fulfilling consequence would be that those same individuals could be targeted. The other dynamic for the expansion of the class of actions subject to lethal force is one which involves pressures placed on operators and members of the U.S. administration to define much more broadly what it means to be a direct participant in hostilities—especially if the detention of indirect participants is foreclosed as an option.

The fifth and last consequence implicates the preservation of discrete rules pertaining to trials. The thought here is fairly straightforward, but it's more speculative. The point is that one shouldn't conflate military trials with detention. If one does, it creates a perverse incentive for decision makers who are responsible for defining fair-trial rights. Whatever rules those individuals design for fair-trial rights, such as defining who may be subject to the jurisdiction of a military court, could spill into detention policies if you conflate the two categories or powers. A better system would be one in which those actors make their decisions exclusively on the basis of procedural rights, balanced against security interests in the trial domain, without having to project what that spillover effect would be in the detention domain. Such a separation also works against opportunism. For example, some individuals who will design or review military trials might strategically define jurisdictional limits or fair-trial rights to effectuate a second-order effect in the detention sphere, and that would also be a mistake. We'd rather want to keep these domains separate and free from such extrinsic considerations.

Finally, let's consider consequences of the proponents' positions. First, their positions might unduly expand the class of actions subject to lethal force. I understand this is a controversial position I'm taking, because some would respond that the pressure placed on expanding the use of lethal force is actually appropriate and beneficial. In my view, however, there's trouble with the ways in which the definition of enemy combatants might be used in the targeting domain. For example, as a thought experiment, take the Military Commissions Act's definition of enemy combatants and think about whether or not those individuals could be lawfully subject to targeting. If you use the definition of enemy combatants under the Military Commissions Act, it might mean that individuals such as faculty and students at U.S. military academies would constitute lawful targets of attack and private military contractors would lose their immunity because the definition conflates the category of indirect participants with combatants and direct participants. In short, it introduces unnecessary if not dangerous confusion into the law of targeting.

Second, some of the proponents' positions undermine counterterrorism efforts. The flip side of the definition of combatancy is the definition of terrorism. It has taken decades for the U.S. Government to obtain international agreement on a definition of terrorism. But the definition of combatancy that has been used in the conflict with al Qaeda introduces ambiguity into the very definition of terrorism that is included in counterterrorism laws, international treaties, and the like. Indeed, the definition of combatants crops, or restricts, the definition of terrorism to a narrower scope of activities. Several international and domestic laws define terrorism to mean violence committed against two groups: "noncombatants" and civilians who do not actively or directly participate in hostilities. Hence, the narrower the definitional boundaries of those two groups is drawn, the wider the range of activities that would not count as terrorism. As an example, let's reverse engineer the definition of terrorism on the basis of the broad definition of combatants adopted by the U.S. Government: it would mean that attacks on the following individuals would not constitute an act of terrorism, that is, attacks on propagandists, financiers, and civilians who provide logistical support to armed forces. Those individuals would no longer technically be covered by the prohibition on terrorism.

A third consequence of the proponents' positions involves a threat to the U.S. legal position on the status of private military contractors. I think this one is very obvious to you all. As you know, the roles

performed by private military contractors are officially deemed not to constitute direct participation in hostility; but those same roles when performed in relationship to al Qaeda are defined as combatancy or direct participation.

A fourth consequence involves a threat to U.S. treaty commitments concerning child soldiers. In the conflict with al Qaeda, a very broad definition of direct participation is being used. In contrast, the U.S. formal position adopted when ratifying the Protocol on Child Soldiers included a very narrow definition of direct participation to make consistent our Government's recruitment, training, and deployment practices. The U.S. Government officially submitted that the phrase "direct participation in hostilities" means "immediate and actual action on the battlefield likely to cause harm to the enemy because there is a direct causal relationship between the activity engaged in and the harm done to the enemy; and does not mean indirect participation in hostilities, such as gathering and transmitting military information, transporting weapons, munitions, or other supplies, or forward deployment." Note that most all of those actions would count as direct participation or satisfy the Military Commissions Act and the Combatant Status Review Tribunal's definition of enemy combatants and very well might satisfy the definition of membership in an armed group under the DoJ's recent memorandum.

Finally, the proponents' positions undermine the fair treatment of differently situated individuals subject to confinement and trial. This point is admittedly speculative. There might be deep normative as well as narrowly pragmatic reasons to differentiate the treatment of civilians who indirectly participate from those who directly participate. We do so, for example, in targeting. And of course, the targeting regime need not have been designed that way. The regime architects could have thought that those individuals are all similarly responsible and should all be subject to lethal force. The question for our purposes is whether those individuals should be treated differently in confinement—and currently they're not—and it's an open question whether the U.S. Government is planning to treat them differently if we do reengage in military trials. But if all those individuals are treated the same way for conditions of confinement, that might be a problem. It's potentially a very serious problem for military trials; that is, if a state cannot lawfully subject a civilian who is an indirect participant in hostilities to a military trial, but the state can lawfully subject a civilian who is a direct participant, those individuals need to be treated differently. Under the system that existed

before the military commissions were suspended, those individuals were all treated the same. Let me elaborate a bit on what transpired. The very widely respected U.N. Special Rapporteur on Counterterrorism and Human Rights criticized the U.S. military commissions for that feature—the very feature of including civilians in the military commissions without admitting to it and without the lawful authority to do so.³⁶ The U.S. Government's reply was, "The United States may not under our law try any civilian before a military commission. Rather, jurisdiction is limited to unlawful enemy combatants. As a result, we question whether speculation about an individual being misclassified warranted inclusion in the [U.N.] report."³⁷ But that begs the question of what is meant by an enemy combatant. If an enemy combatant is a civilian who indirectly participates in hostilities, then we're back to the same question. So my parting thought for this set of concerns is that only time will tell whether the DoJ's memorandum pursues the same line or is really a different framework with respect to the classification of one or two groups of actors in these contexts.

In conclusion, one way to end my opening remarks is just to say that some of the best legal minds, including in this audience, are now trying to figure out the answer to these various questions. These are really difficult problems. The Judiciary, the Executive Branch, Congress, and legal advocates now have an opportunity to decide how to align U.S. discourse and policy with the long-standing international legal framework. My hope is that we'll ultimately design rules that consider the integrity of the law of armed conflict regime not only in the current conflict but for prospective ones as well. If we do not, we will jeopardize both humanitarian and security interests now and in the future.

Thank you very much for this opportunity.

³⁶ U.N. Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, ¶ 30, U.N. Doc. A/HRC/6/17/Add.3 (Nov. 22, 2007) (*prepared by* Martin Scheinin).

³⁷ U.S. Diplomatic Mission to the U.N. in Geneva, United States Comments on the Report on the Mission to the United States of America of the Special Rapporteur on the Protection and Promotion of Human Rights and Fundamental Freedoms While Countering Terrorism, ¶ 30 (*prepared by* Martin Scheinin), *available at* <http://geneva.usmission.gov/Press2007/Scheinin-Response-HRC.pdf>.

Appendix A**Category Mistakes*****Type 1: Actor conflation***

Grouping different actors under a heading that correctly applies only to some of them

Example: defining “combatants” to include civilians who do not directly participate in hostilities

Type 2: Actor disaggregation

Failure to recognize when distinct categories of individuals are all lawfully subject to the same coercive measure

Example: contending that parties may target regular armed forces but not civilians who directly participate in hostilities

Type 3: Power conflation

Grouping distinct coercive powers under a heading that correctly applies only to some of them

Example: assuming that a prohibition on military trials (the greater power) means that the prohibition applies to military detention (the lesser power) as well

Appendix B

Definitions of “Enemy Combatants” and Detainable Individuals

I. U.S. Department of Defense, Fact Sheet (February 2004)

“At the time of capture and based on available information, combatant and field commanders determine whether a captured individual was part of or supporting forces hostile to the United States or coalition partners, and engaged in an armed conflict against the United States. Such persons are enemy combatants.”

II. Hamdi v. Rumsfeld, 542 U.S. 507 (March 2004) (plurality opinion)

“an individual who . . . was ‘part of or supporting forces hostile to the United States or coalition partners’ in Afghanistan and who ‘engaged in an armed conflict against the United States’ there.”

III: Combatant Status Review Tribunals (July 2004)

“an individual who was part of or supporting Taliban or al Qaeda forces, or associated forces that are engaged in hostilities against the United States or its coalition partners.”

IV: Military Commissions Act (Dec. 2006)

“‘unlawful enemy combatant’ means . . . a person who has engaged in hostilities or who has purposefully and materially supported hostilities against the United States or its co-belligerents who is not a lawful enemy combatant (including a person who is part of the Taliban, al Qaeda, or associated forces).”

V. U.S. Department of Justice (March 2009)

“The President has the authority to detain persons that the President determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, and persons who harbored those responsible for those attacks. The President also has the authority to detain persons who were part of, or substantially supported, Taliban or al-Qaida forces or associated forces that are engaged in hostilities against the United States or its coalition partners, including any person who has committed a belligerent act, or has directly supported hostilities, in aid of such enemy armed forces.”

SWAY: THE IRRESISTIBLE PULL OF IRRATIONAL BEHAVIOR¹REVIEWED BY MAJOR MICHAEL D. O'NEILL²

“What I tell you three times is true.”³ This line from a Lewis Carroll story largely sums up the cautionary tale behind *Sway: The Irresistible Pull of Irrational Behavior*, a book by Ori Brafman and his brother, Rom Brafman. Plucking from a myriad of anecdotal and scientific evidence, these two brothers attempt to persuade, or “sway,” the reader into believing that even the most capable of minds are all too willing to accept perception over reality whenever emotions are involved.⁴ This is the “irrational” behavior noted in the book’s title. I would contend, however, that much of what the authors term irrational is, in fact, quite rational in a world of limited facts and functional necessity. If we did not act on our perceived realities and instincts, our world would come to a screeching halt.

The Brafman brothers are not new to the study of human behavior. Ori is a self-proclaimed “organizational expert” and his brother Rom holds a doctorate in psychology.⁵ This book is not, however, an original study by the brothers. Rather, *Sway* gathers a broad range of behavioral studies performed by others and presents them with simple summaries, free of scientific jargon and complexity. While not perfect, *Sway* is a quick and enjoyable read that provides several keen insights for anyone called upon to lead, manage, or counsel. Whether you are a parent or a staff judge advocate, you would be wise to allow some sway in your beliefs regarding how you interact with others and how you process your daily judgments.

Sway states its purpose up front. It is intended to make the reader reflect on our natural tendencies to quickly “label a person or a situation.”⁶ Once labeled, according to the authors, we will have shackled ourselves to that initial perception which then becomes our

¹ ORI BRAFMAN & ROM BRAFMAN, *SWAY, THE IRRESISTIBLE PULL OF IRRATIONAL BEHAVIOR* (2008).

² U.S. Army. Written while assigned as a student, 57th Judge Advocate Officer Graduate Course, The Judge Advocate Gen.’s Legal Ctr. & Sch., U.S. Army, Charlottesville, Va.

³ LEWIS CARROLL, *THE HUNTING OF THE SNARK* 4 (1876).

⁴ BRAFMAN & BRAFMAN, *supra* note 1, at 22.

⁵ *Id.* at inside back cover.

⁶ *Id.* at 7.

reality; objectivity is lost and irrational thoughts can win the day. The Brafman brothers assert that virtually all of our daily judgments are influenced by this “irrational” bias.⁷

The authors never clearly define what it means to be “irrational” in this context, but it is clear that any decision tainted by emotion or bias could fall into that category.⁸ We must assume, in contrast, that a “rational” decision is the type of decision that would be made by an intelligent computer or Mr. Spock from *Star Trek* fame.⁹ One could argue that much of what the authors label as “irrational” is merely risk-taking gone bad. I would suggest that, had the risk-takers succeeded, we would praise their judgment, rather than label it “irrational.”

Sway begins the way it ends, by introducing the reader to a wide range of counterintuitive case studies performed over the years. These studies typically fall into two broad categories: hindsight analysis of real life decision making or academic experiments with unwitting subjects and control groups.¹⁰ What most of these studies have in common is the advantage of being detached from the emotional decision-making process experienced by the subjects of the study. By looking in from afar, the observers can avoid the emotional ties that have driven a particular decision. No matter the reader’s opinion on this type of second guessing, the outcome of these experiments will likely be a surprise.

Most startling were the studies that showed how powerful a placebo effect can be. A placebo effect is the “beneficial effect in a patient following a treatment that arises from the patient’s expectations concerning the treatment rather than from the treatment itself.”¹¹ The placebo cited in *Sway* was not a sugar pill substituted for a prescription drug, but false information passed off as authentic to the test subjects.¹² As with drug placebos, informational placebos seem to tap into the healing power of the human mind. *Sway* introduces the reader to a new

⁷ *Id.* at 180.

⁸ See generally *id.* at 6 (discussing the effect of “diagnosis bias” experienced by emergency room doctors when dealing with the same patients day after day).

⁹ When Mr. Spock was able to suppress his half-human side and rely on his logic-driven Vulcan side. See *Star Trek* (NBC television broadcast Sept. 8, 1966–Sept. 2, 1969).

¹⁰ See generally BRAFMAN & BRAFMAN, *supra* note 1, at 9–24 (discussing an aircraft collision and experiments with customers buying eggs).

¹¹ WEBSTER II, *NEW COLLEGE DICTIONARY* 861 (3d ed. 2005).

¹² See BRAFMAN & BRAFMAN, *supra* note 1, at 97.

twist on the placebo effect—namely, the potential influence of simply being told that you are either elite or substandard without any objective basis for doing so.

The authors label this effect “value attribution.” If the studies presented are to be believed, “value attribution” not only engenders bias in the attributor, but enhances or detracts from the actual performance of the subject of the attribution.¹³ In other words, simply being identified as elite can cause the subject to perform at higher levels on an objective test than he or she may have otherwise.¹⁴ In the reverse, being identified as substandard may cause subjects to perform worse.¹⁵

One given example of such an “attribution” effect involved Israeli soldiers who were randomly identified to their new military trainers as having “command potential” that was “high, regular,” or “unknown.”¹⁶ Neither the trainees nor their trainers had any knowledge that the designations were phony, but after fifteen weeks of training, those identified as having higher command potential performed “much better” on diagnostic tests.¹⁷ This type of study highlights what has been called the “Pygmalion effect”: higher expectations lead to higher levels of measurable performance.¹⁸

The Pygmalion effect is fascinating because it has the potential to provide a simple mechanism for any group leader to increase performance levels. It also raises questions as to what really drives one group to perform in a superior fashion as compared to others. Is it the training or the reputation? Are U.S. Marines renowned warriors because of their training or simply because that is what is expected of them? Are U.S. Army Rangers really more capable than Regular Army infantry, or are they just trying to live up to their reputation?

All group leaders should take this effect into account when communicating with subordinates. Set high expectations and stroke egos. According to the Brafmans, if you consistently tell subordinates that they are “the best,” they will likely come to believe it. The same lesson can be applied to child rearing, as well. Foster a positive sense of

¹³ *Id.* at 55.

¹⁴ *See id.* at 99.

¹⁵ *Id.*

¹⁶ *Id.* at 98.

¹⁷ *Id.* at 99.

¹⁸ *See generally id.* at 97 (referencing multiple studies on the Pygmalion effect).

self-worth in your children and you may create a self-fulfilling prophecy. This, of course, raises the question as to what kinds of praise—or derision—will have the greatest effect. There is also some evidence that not all “value attributions” will have a similar effect. The phenomena outlined in *Sway* seem, in fact, to run counter to the findings in another book that has drawn favorable comparisons: *Freakonomics*.¹⁹

Chapter six in *Freakonomics* explores the effect of children’s names on their development. In one case, a father named two of his sons “Winner” and “Loser.”²⁰ Applying the Pygmalion effect, “Winner” should have led a more successful life than “Loser.” Just the opposite turned out to be true, however; “Winner” was a loser and “Loser” was a winner.²¹ How could this happen? Although this study seems to conflict with *Sway*, the two findings may not be as incompatible as they may seem. *Sway* focuses on what types of expectations are placed on a child or individual. It is unclear that someone’s name alone sets other’s expectations. More likely, other personality factors would quickly overcome any preconceptions associated with one’s name.

Sway also highlights our human need to feel that we have been treated fairly in our dealings with others. As the authors point out, “[w]e don’t typically think of fairness as an irrational force, but it dramatically affects our perceptions and sways our thinking.”²² According to the cited studies, “when it comes to fairness, it is the *process*, not the *outcome*, that causes us to act irrationally.”²³ In this context, clients could be considered “irrational” if they are fully satisfied with a service, in spite of not receiving what would objectively appear to be the best possible outcome.²⁴

One would think, for example, that a convicted felon would be bitter about the process that put him in prison, but *Sway* tells us this is not always the case. In surveys with convicted felons, researchers found that the time spent with their lawyers mattered greatly in shaping whether the criminals felt that they were treated fairly.²⁵ This was true “regardless of

¹⁹ *Id.* at back cover (“A breathtaking book that will challenge your every thought, *Sway* hovers above the intersection of *Blink* and *Freakonomics*.”).

²⁰ STEVEN D. LEVIT & STEPHEN J. DUBNER, *FREAKONOMICS* 179 (2005).

²¹ *Id.* at 180.

²² BRAFMAN & BRAFMAN, *supra* note 1, at 128.

²³ *Id.* at 118 (emphasis added).

²⁴ *Id.* at 120–21.

²⁵ *Id.* at 120.

the crime they committed or the punishment they received.”²⁶ Here we see the importance of due process in practice, not simply in name.

This concept is crucial for every attorney, judge, or military leader to be aware of because it goes to the heart of unit morale and discipline. The lesson here is that commanders and their legal advisors need to ensure that military discipline is exercised in ways that are perceived to be fair, consistent, and predictable. Soldiers must feel that they have a voice and that their voices have been heard. Likewise, military attorneys should make special efforts when communicating with their clients. Whether we are talking about informal counseling or courts-martial, the process often matters more than the outcome.

This philosophy is formally acknowledged in the Army Command Policy regulation, which states:

In addition to being mentally, physically, tactically, and technically competent, Soldiers must have confidence in themselves, their equipment, their peers, and their leaders. A leadership climate in which all Soldiers are treated with *fairness, justice, and equity* will be crucial to development of this confidence within Soldiers. Commanders are responsible for developing disciplined and cohesive units sustained at the highest readiness level possible.²⁷

Such fairness in process extends beyond military discipline, as well. Fairness must also be applied to work evaluations, group plans, and projects. To that end, frequent assessments of progress and communication among members of a team can minimize feelings of uncertainty and surprise. This can be accomplished during the often overlooked performance counseling session.²⁸ As the authors put it, “rather than assuming the final product speaks for itself, it’s good to remember to regularly engage and update members of our team during the process.”²⁹ It seems that regular counseling may serve a useful purpose, after all, for those who had any doubts.

²⁶ *Id.*

²⁷ U.S. DEP’T OF ARMY, REG. 600-20, ARMY COMMAND POLICY para. 1-5c(4)(c) (18 Mar. 2008) (emphasis added).

²⁸ *Id.* para. 2-3.

²⁹ BRAFMAN & BRAFMAN, *supra* note 1, at 129.

Another important lesson to take from *Sway* involves the positive impact of dissent in a group environment. Although the power of peer pressure is well-known, the authors point out how easily those pressures can be relieved by just a single “dissenting voice.”³⁰ Such a voice gives others in the group an avenue to open up and share their own opinions.³¹ This kind of dissent is crucial to the free flow of ideas in any small group environment. The “sway of group conformity” is very strong, but the studies provided show that any expressed counter-view, right or wrong, is often enough to break the grip of this irrational behavior.³² The message in the military environment is to empower your staff to speak up and express their views, no matter how trivial they may seem. Rank or position must not inhibit contribution from all team members.

Sway is not without its faults, however. Many of the so-called “irrational” pulls are simply gambles that did not pay off. Is it always “irrational” to gamble? I would say no. The authors note that the University of Florida football program excelled in the 1990s because its new head coach, Steve Spurrier, was not afraid to play an aggressive “Fun-n-Gun” offense against more conservative coaches who were “playing not to lose.”³³ The authors praise Spurrier for not being sucked into the “sway” of a loss aversion mentality, but had his offense failed, I must believe that the authors would be accusing him of an irrational emotional investment in a losing behavior.³⁴

The authors made this accusation when presenting the case of an ill-fated decision (or gamble) by an experienced KLM pilot who broke with normal procedures and attempted to take off in the fog without waiting for a final clearance from the tower.³⁵ That decision ultimately resulted in the deaths of hundreds of passengers and aircrew when the pilot’s Boeing 747 slammed into another taxiing 747 that had not yet cleared the runway.³⁶ The authors focused heavily on the fact that the pilot was preoccupied by an overriding concern about previous delays and the costs associated with another extended delay.³⁷ Thus, the authors

³⁰ *Id.* at 155.

³¹ *Id.*

³² *Id.* at 154.

³³ *Id.* at 28.

³⁴ *Id.* at 30 (noting that “aversion to loss” is a “powerful” force that causes individuals to avoid change and to “[stay] the course”).

³⁵ *Id.* at 11–16.

³⁶ *Id.* at 15.

³⁷ *Id.* at 11–12.

conclude, the pilot acted irrationally.³⁸

The other side of the argument is that an experienced pilot took what he perceived at the time to be a relatively small risk. He likely assessed that the odds of another aircraft taxiing on the same runway were so slim as to be irrelevant. Had the pilot been correct, he may have avoided a further lengthy delay due to fog. The pilot, in this case, was the experienced head of KLM's safety program.³⁹ He was widely regarded as a "methodical" professional with a "spotless [safety] record."⁴⁰ If this professional pilot carried a burden of "loss aversion," it is just as likely that he had an aversion to breaking from established flight procedures as he did to incurring further flight delays.

Viewed from this perspective, the only significant difference between the two risk scenarios is that Spurrier succeeded while the KLM pilot failed. This implies that risk-takers who fail have, by definition, been influenced by an "irrational pull." It seems the authors want it both ways. The reader is told that when we break free from the "pull" of conservative loss aversion and succeed (like Steve Spurrier) we will be rewarded, but when we break free from the "pull" of conservative loss aversion and fail (like the KLM pilot) we have displayed an irrational, emotional weakness.

The reality is that quick decisions made with limited facts are a rational necessity in our daily lives as a matter of efficiency. This concept is explored in more detail in *Blink*, a book by Malcolm Gladwell.⁴¹ In what could be considered a counterpoint to *Sway*, *Blink*, distinguishes between our "conscious and unconscious modes of thinking."⁴² In short, our "conscious" decisions are those decisions made with some forethought, while our "unconscious" decisions are much more "spontaneous" in nature.⁴³ *Blink* goes so far as to defend quick decisions as "every bit as good as decisions made cautiously and deliberately."⁴⁴

³⁸ See *id.* at 21 ("he tuned out . . . his common sense and years of training").

³⁹ *Id.* at 10.

⁴⁰ *Id.*

⁴¹ See MALCOLM GLADWELL, *BLINK, THE POWER OF THINKING WITHOUT THINKING* (2005).

⁴² *Id.* at 12 (citing psychologist Timothy D. Wilson).

⁴³ *Id.*

⁴⁴ *Id.* at 14.

This is possible because our unconscious decisions are not made without thought; they are simply calculated beneath a level of conscious recognition.⁴⁵ Interestingly, *Blink* points out that *more* information is not necessarily better.⁴⁶ The author recounts an experiment involving a group of psychologists who were asked to diagnose the case of a “war veteran.”⁴⁷ Those psychologists took repeated diagnostic tests concerning the veteran with varying levels of information for each test.⁴⁸ Initially, the psychologists had very little information to work with, but their early diagnoses proved to be just as accurate as their later diagnoses made with much more information.⁴⁹ The only real difference between the early and later diagnoses was the level of confidence felt by the individuals making them—their confidence increased, even though the accuracy of their diagnoses remained the same.⁵⁰ It is a weakness in *Sway* to label impulsive decisions as irrational when they lead to failure versus success.

Despite this shortcoming, *Sway* excels in making the reader think about the power of human perception. It is a book that works best when it delves into the positive effects of value attribution, fair process, and group dynamics.⁵¹ In these contexts, our human tendency to “irrationally” accept and act upon perception over reality can be a plus when properly fostered and applied. Leaders of all types should tap into this natural force by repeatedly reminding their teams of their special attributes. *Sway* also surprises in its exploration of process over outcome and the value of dissent.⁵² Lawyers should realize that if simply spending a few minutes of additional time with a client can alter the client’s perception of how he was treated, then that time is well spent.

This reviewer doubts, however, that our human inclination to take risks will ever change, nor is it clear that the authors are expecting as much.⁵³ As a practical matter, humans must frequently act on less than full and accurate information. When we do, we have to invoke our “gut”

⁴⁵ See *id.* at 70.

⁴⁶ See *id.* at 139.

⁴⁷ *Id.*

⁴⁸ *Id.*

⁴⁹ See *id.* at 140.

⁵⁰ *Id.*

⁵¹ See BRAFMAN & BRAFMAN, *supra* note 1, at 55, 120.

⁵² See *id.* at 155.

⁵³ See *id.* at 88 (noting that knowledge of attribution bias is often insufficient to cause changes in process).

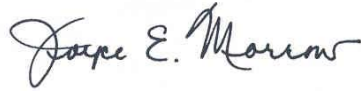
instincts and emotions to fill the informational gap. The authors seem to view these informational shortcuts as “rational” or “irrational” depending on the ultimate outcome. But, without the benefit of hindsight, the incorporation of emotion into our daily judgment is quite rational and often accurate.⁵⁴ That is exactly why its pull is so irresistible.

⁵⁴ See GLADWELL, *supra* note 41, at 14.

By Order of the Secretary of the Army:

GEORGE W. CASEY, JR.
General, United States Army
Chief of Staff

Official:

A handwritten signature in cursive script that reads "Joyce E. Morrow".

JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army
0928804

