

# NATIONAL SECURITY & ARMED CONFLICT LAW REVIEW

Volume III

Fall 2013

2013–2014

## EXECUTIVE BOARD

COREY P. GRAY

*Editor in Chief*

PAIGE E. REESE

*Senior Articles Editor*

DAVID A. ROLLER

*Executive Managing  
Editor*

JAMES M. SLATER

*Senior Notes  
Editor*

MICHAEL J. WEISS

*Senior Symposium Editor*

TIMOTHY J. GREEN

*Senior Online  
Editor*

## EDITORIAL BOARD

Krysta Ku

*Senior Articles Editor*

Rebecca Beaudoin

Jared E. Dallau

Nicholas H. Esser

Sarah E. Fowler

Brian M. Heit

Jerome A. Jackson

Daniel P. Kinney

James Klein

Michael J. Kranzler

John M. Moscarino

Noel C. Pace

Christopher N. Pawlik

Marc E. Rosenthal

Claire L. Rumler

Jessica Sblendorio

Laura E. Scala

Michael W. Thicksten

Jonathan A. Stamm

*Senior Articles Editor*

Zachary H. Ward

*Senior Articles Editor*

PROFESSOR MARKUS WAGNER

*Faculty Advisor*

GLORIA GARCIA

*Administrative Assistant*

EMILY HOROWITZ

*Administrative Assistant*



# UNIVERSITY OF MIAMI SCHOOL OF LAW

## ADMINISTRATION

Donna E. Shalala, B.A., Ph.D., *President of the University*  
Thomas J. LeBlanc, B.S., M.S., Ph.D., *Provost & Executive Vice President*  
Patricia D. White, B.A., M.A., J.D., *Dean & Professor of Law*  
Patrick O. Gudridge, A.B., J.D., *Vice Dean & Professor of Law*  
Ileana Porras, B.A., M.Phil., J.D., *Associate Dean of Academic Affairs*  
Raquel M. Matas, B.A., J.D., *Associate Dean for Administration and Counsel to the Dean*  
Douglas K. Bischoff, A.B., J.D., LL.M., *Associate Dean for the Adjunct Faculty & Director of the Graduate Program in Real Property Development*  
Georgina Angones, B.A., *Assistant Dean for Law Development and Alumni Relations*  
Marcelyn Cox, B.A., J.D., *Assistant Dean, Career Development Office*  
Michael L. Goodnight, B.A., M.S., *Associate Dean of Admissions and Enrollment Management*  
Janet E. Stearns, B.A., J.D., *Dean of Students*  
Marni B. Lennon, B.A., Ms.Ed., J.D., *Assistant Dean for Public Interest and Pro Bono, Director, HOPE Public Interest Resource Center*  
William P. VanderWyden, III, B.A., M.Ed., J.D., *Assistant Dean for Professional Development*  
Greg Levy, B.A., J.D., *Assistant Dean of Academic Affairs and Student Services*

## FACULTY

David Abraham, B.A., M.A., Ph.D., J.D., *Professor of Law & University of Miami Law Review Faculty Advisor*  
Anthony V. Alfieri, A.B., J.D., *Dean's Distinguished Scholar, Professor of Law & Director of the Center for Ethics & Public Service*  
Paula Arias, J.D., *Director of International Moot Court Program & Lecturer in Law*  
Jill Barton, B.J., B.A., M.S., J.D., *Lecturer in Law*  
Ricardo Bascuas, B.A., J.D., *Professor of Law*  
Ellen Belfer, B.A., J.D., *Lecturer in Law*  
Caroline Bettinger-Lopez, B.A., J.D., *Associate Professor of Clinical Legal Education & Director, Human Rights Clinic*  
William Blatt, A.B., J.D., *Professor of Law*  
Caroline M. Bradley, B.A. (Hons), LL.M., *Professor of Law*  
Patricia A. Brown, B.S.F.S., J.D., *Director, Graduate Program in Taxation*  
Sergio Campos, A.B., J.D., *Associate Professor of Law*  
Donna K. Coker, B.S.W., M.S.W., J.D., *Professor of Law*  
Mary I. Coombs, B.A., M.A., J.D., *Professor of Law*  
Charlton Copeland, B.A., M.A.R., J.D., *Professor of Law*  
Caroline Mala Corbin, B.A., J.D., *Professor of Law*  
Andrew Dawson, B.A., J.D., *Associate Professor of Law*  
Michele DeStefano, B.A., J.D., *Associate Professor of Law*  
Stephen M. Diamond, B.A., A.M., Ph.D., J.D., *Professor of Law*  
Mary Teresa Doud, B.A., M.A., J.D., *Lecturer in Law*  
Mary Doyle, B.A., LL.B., *Dean Emerita & Professor of Law*  
Alyssa Dragnich, B.A., J.D., *Lecturer in Law*  
Marc Fajer, A.B., J.D., *Professor of Law*  
Zanita E. Fenton, A.B., J.D., *Professor of Law*  
Mary Anne Franks, B.A., M.Phil., Ph.D., J.D., *Associate Professor of Law*

Christina M. Frohock, B.A., M.A., J.D., *Lecturer in Law*

A. Michael Froomkin, B.A., M.Phil., J.D., *Laurie Silvers and Mitchell Rubenstein Distinguished Professor of Law*

Michael H. Graham, B.S.E., J.D., *Dean's Distinguished Scholar for the Profession, Professor of Law*

Susan Haack, B.A., M.A., B.Phil., Ph.D., *Distinguished Professor in the Humanities, Cooper Senior Scholar in Arts and Sciences, Professor of Philosophy & Professor of Law*

Stephen K. Halpert, A.B., J.D., *Professor of Law*

Frances R. Hill, B.A., M.A., Ph.D., J.D., LL.M., *Dean's Distinguished Scholar for the Profession, Professor of Law*

Jennifer Hill, B.A., M.A., J.D., *Lecturer in Law*

Elizabeth M. Iglesias, B.A., J.D., *Professor of Law*

Jan L. Jacobowitz, B.S., J.D., *Director of the Professional Responsibility and Ethics Program & Lecturer in Law*

Osamudia James, B.A., J.D., LL.M., *Associate Professor of Law*

D. Marvin Jones, B.S., J.D., *Professor of Law*

Stanley I. Langbein, A.B., J.D., *Professor of Law*

Tamara Rice Lave, B.A., M.A., Ph.D., J.D., *Associate Professor of Law*

Lili Levi, A.B., J.D., *Professor of Law*

Dennis O. Lynch, B.A., J.D., J.S.D., LL.M., *Dean Emeritus & Professor of Law*

Martha R. Mahoney, B.A., M.A., J.D., *Professor of Law*

Elliott Manning, A.B., J.D., *Dean's Distinguished Scholar for the Profession, Professor of Law*

Fred McChesney, A.B., J.D., Ph.D., *Carlos de la Cruz-Soia Mentschikoff Chair in Law and Economics*

Felix Mormann, J.D., LL.M., *Associate Professor of Law*

Jessica Carvalho Morris, J.D., *Director of International Graduate Law Programs*

Sarah A. Mourer, B.S., J.D., *Director of the Capital Defense Project and Miami Innocence Project & Associate Professor of Clinical Legal Education*

George Mundstock, B.A., J.D., *Professor of Law*

Peter Nemerovski, B.A., J.D., *Lecturer in Law*

JoNel Newman, B.A., J.D., *Director of the Health and Elder Law Clinic & Professor of Clinical Legal Education*

James W. Nickel, B.A., Ph.D., *Professor of Philosophy & Professor of Law*

Leigh Osofsky, A.B., J.D., *Associate Professor of Law*

Bernard H. Oxman, A.B., J.D., *Richard A. Hausler Endowed Chair & Professor of Law*

Kunal Parker, A.B., M.A., J.D., Ph.D., *Dean's Distinguished Scholar & Professor of Law*

Jan Paulsson, A.B., J.D., *Michael Klein Distinguished Scholar Chair & Professor of Law*

Bernard P. Perlmutter, B.A., J.D., *Director of the Children & Youth Law Clinic & Professor of Clinical Legal Education*

Shara Pelz, B.A., J.D., *Lecturer in Law*

Alejandro Portes, B.A., M.A., Ph.D., *Professor of Sociology & Professor of Law*

Tina Portuondo, B.A., J.D., LL.M., *Director of the Heckerling Institute on Estate Planning*

Thomas A. Robinson, B.S., J.D., B.Litt., *Professor of Law*

Scott Rogers, B.S., M.S., J.D., *Director, Mindfulness and the Law Program & Lecturer in Law*

Laurence M. Rose, B.A., J.D., *Director of the Litigation Skills Program & Professor of Law Emeritus*

Robert E. Rosen, A.B., M.A., J.D., Ph.D., *Professor of Law*

Keith S. Rosenn, B.A., LL.B., *Professor of Law & Chair of Foreign Graduate Law Program*

Edgardo Rotman, J.D., LL.M., Ph.D., LL.B., *Lecturer in International & Comparative Law*

Andres Sawicki, S.B., J.D., *Associate Professor of Law*  
Stephen J. Schnably, A.B., J.D., *Professor of Law*  
Rebecca Sharpless, B.A., M.Phil., J.D., *Associate Professor of Clinical Legal Education*  
Rachel Smith, B.A., J.D., *Lecturer in Law*  
Rachel Stabler, B.A., J.D., *Lecturer in Law*  
Kele Stewart, B.S., J.D., *Professor of Clinical Legal Education*  
Irwin P. Stotzky, B.A., J.D., *Professor of Law*  
Scott Sundby, B.A., J.D., *Dean's Distinguished Scholar & Professor of Law*  
Jessi Tamayo, B.A., J.D., *Director of Public Programming & Lecturer in Law*  
Annette Torres, B.A., M.B.A., J.D., *Lecturer in Law*  
Stephen K. Urice, B.A., Ph.D., J.D., *Professor of Law*  
Francisco Valdes, B.A., J.D., J.S.M., J.S.D., *Dean's Distinguished Scholar & Professor of Law*  
Teresa Verges, B.A. J.D., *Director, Investor Rights Clinic & Lecturer in Law*  
Markus Wagner, J.S.M., M.J.I., J.D., *Associate Professor of Law*  
William H. Widen, A.B., J.D., *Professor of Law*  
Richard L. Williamson, Jr., A.B., M.A., J.D., *Professor of Law*  
Sally H. Wise, B.A., J.D., M.LL., *Director of the Law Library & Professor of Law*  
Jennifer H. Zawid, B.A., J.D., *Director of the Externship Program & Lecturer in Law*  
Cheryl Zuckerman, B.A., J.D., *Lecturer in Law*

#### **Emeriti**

Terence J. Anderson, B.A., J.D., *Professor Emeritus of Law*  
Kenneth M. Casebeer, A.B., J.D., *Professor Emeritus of Law*  
M. Minnette Massey, B.B.A., LL.B., M.A., LL.M., *Professor Emerita of Law*  
Kathryn D. Sowle, B.A., J.D., *Professor Emerita of Law*

#### **Visiting Professors**

Kristina Klykova, LL.M., *Visiting Assistant Professor*





# NATIONAL SECURITY & ARMED CONFLICT LAW REVIEW

Volume III

Fall

2013–2014

## ARTICLES

I.	THE EYES OF THE WORLD: CHARGES, CHALLENGES, AND GUANTÁNAMO MILITARY COMMISSIONS AFTER HAMDAN II.....	<i>Christina M. Frohock</i>	7
II.	NON-STATE ARMED GROUPS AND TECHNOLOGY: THE HUMANITARIAN TRAGEDY AT OUR DOORSTEP?.....	<i>Colonel Dave Wallace</i> & <i>Major Shane Reeves</i>	26
III.	SUN TZU’S BATTLE FOR YOUR FOOTNOTES: THE EMERGENT ROLE OF LIBRARIES IN JUDICIAL WARFARE.....	<i>Mark McCary</i>	46
IV.	LAW AS SHIELD, LAW AS SWORD: THE ICC’S <i>LUBANGA</i> DECISION, CHILD SOLDIERS AND THE PERVERSE MUTUALISM OF PARTICIPATION IN HOSTILITIES .....	<i>Chris Jenks</i>	106

## NOTES

I.	SEPARATE BUT EQUAL ACCOUNTABILITY: THE CASE OF OMAR KHADR.....	<i>Grantland Lyons</i>	125
II.	CYBER UTILITIES INFRASTRUCTURE AND GOVERNMENT CONTRACTING .....	<i>Corey P. Gray</i>	151
III.	THE APPLICATION OF THE ADMINISTRATIVE PROCEDURE ACT TO PRIVATE-PUBLIC SECTOR PARTNERSHIPS IN HOMELAND SECURITY.....	<i>Michael James Weiss</i>	172

## BOOK REVIEW

IV.	TERRORISM, TICKING TIME-BOMBS, AND TORTURE: A PHILOSOPHICAL ANALYSIS .....	<i>By Fritz Allhoff</i> <i>Reviewed by Krysta Ku</i>	195
-----	---	---	-----



## Acknowledgements

The editors thank Markus Wagner, Janet E. Stearns, Emily Horowitz, Gloria Garcia, Robin Schard, Pam Lucken, Roland Liwag, Ana Ramirez, The Sheridan Press, and the University of Miami School of Law for their generous contributions of leadership, guidance and support, without which the digital and print journal would not have been possible.



ARTICLE

The Eyes of the World:  
Charges, Challenges, and Guantánamo Military  
Commissions After *Hamdan II*

Christina M. Frohock\*

Abstract

*Guantánamo military commissions are under a spotlight, scrutinized by the judiciary and the public. Just the word “Guantánamo” can trigger impassioned reactions from both advocates and detractors. This Article takes a measured view, examining a recent opinion from the U.S. Court of Appeals for the D.C. Circuit, Hamdan v. United States (“Hamdan II”), that speaks to the legitimacy of military commissions convened in Guantánamo to try the September 11th defendants and others. While several media commentators seized on the opinion as striking a blow to Guantánamo proceedings, in fact the opinion approves military commissions and offers a roadmap for prosecutors. After describing the history of Hamdan II, this Article shows how the opinion reaches terrorism cases in both military commissions and federal courts.*

Table of Contents

---

I. INTRODUCTION.....	8
II. THE <i>HAMDAN</i> OPINIONS .....	9
III. THE IMPACT OF <i>HAMDAN II</i> ON MILITARY COMMISSIONS.....	14
IV. THE REACH OF <i>HAMDAN II</i> BEYOND MILITARY COMMISSIONS.....	20
V. CONCLUSION.....	25

---

\* Lecturer in Law, University of Miami School of Law; J.D. *magna cum laude*, New York University School of Law; M.A., University of Michigan; B.A., University of North Carolina. My thanks to Joel Feigenbaum and Tricia Robinson for their editorial support and to Allison Brede for her tireless research.

## I. INTRODUCTION

The use of military commissions to try alleged terrorists in Guantánamo Bay, Cuba, has attracted worldwide scrutiny. A military commission is a court convened before a military judge rather than an Article III judge, designed to try individuals accused of offenses during war.<sup>1</sup> The United States relies on such trials in the armed conflict against al Qaeda and associated forces,<sup>2</sup> and the current trial in Guantánamo for the September 11th attacks has intensified the political debate and public criticism of this form of justice.<sup>3</sup> But not every voice is undermining. The U.S. Court of Appeals for the D.C. Circuit recently spoke in *Hamdan v. United States* (“*Hamdan II*”),<sup>4</sup> an opinion that both legitimates Guantánamo military commissions and offers guidance in terrorism cases more broadly.

This Article sets *Hamdan II* against the backdrop of the U.S. Supreme Court’s prior opinion in *Hamdan v. Rumsfeld* (“*Hamdan I*”),<sup>5</sup> describing the progression of cases involving Guantánamo detainee Salim Ahmed Hamdan. Next, the Article argues that, contrary to its occasionally sensationalist portrayal in the media, the D.C. Circuit Court’s opinion invites further military commissions and offers a roadmap for the proceedings. Certain charges, including “providing material support for terrorism,” are available for conduct only after enactment of the Military Commissions Act (“MCA”) of 2006, as

---

<sup>1</sup> See JENNIFER ELSEA, CONG. RESEARCH SERV., R41163, THE MILITARY COMMISSIONS ACT OF 2009: OVERVIEW AND LEGAL ISSUES 4 (2010).

<sup>2</sup> Military commissions have a long history and were an early component of the United States’ response to the September 11th attacks. See Military Order of Nov. 13, 2001: Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terrorism, 66 Fed. Reg. 57,833 § 1(e) (Nov. 16, 2001) [hereinafter Military Order]; George W. Bush, Remarks by the President on National Security, Speech at National Archives (May 21, 2009) (“Military commissions have a history in the United States dating back to George Washington and the Revolutionary War. They are an appropriate venue for trying detainees for violations of the laws of war.”); GUANTÁNAMO REVIEW TASK FORCE, FINAL REPORT 19 (2010).

<sup>3</sup> See, e.g., U.S. GOV’T ACCOUNTING OFFICE, GAO 13-31, GUANTÁNAMO BAY DETAINEES: FACILITIES AND FACTORS FOR CONSIDERATION IF DETAINEES WERE BROUGHT TO THE UNITED STATES (2012) [hereinafter GAO REPORT] at 1–4 (transfer study requested by Senator Dianne Feinstein); Andrea Prasow, *A Failed Experiment*, N.Y. TIMES, Nov. 19, 2012, <http://www.nytimes.com/roomfordebate/2012/11/18/should-obama-close-guantanamo-and-end-military-tribunals/close-guantanamo-and-stop-the-military-commissions> (“The system lacked fundamental protections required for fair trials.”); Laura Pitter, *Guantánamo’s System of Injustice*, SALON (Jan. 19, 2012), [http://www.salon.com/2012/01/19/guantanamos\\_system\\_of\\_injustice/](http://www.salon.com/2012/01/19/guantanamos_system_of_injustice/) (“The US does not need to use this fundamentally flawed military commission system.”).

<sup>4</sup> 696 F.3d 1238 (D.C. Cir. 2012).

<sup>5</sup> 548 U.S. 557 (2006).

revised in 2009.<sup>6</sup> Finally, the Article argues that *Hamdan II* reaches beyond military commissions and suggests constitutional challenges in federal cases outside the MCA.

“The eyes of the world are on Guantánamo Bay,” observed one district court judge who ruled on Hamdan’s filings for several years.<sup>7</sup> *Hamdan II* provides a new lens through which the world may view military commissions and terrorism cases.

## II. THE *HAMDAN* OPINIONS

The attacks of September 11, 2001, “created a state of armed conflict,” in the words of then-President George W. Bush.<sup>8</sup> One week after the attacks, Congress passed its Authorization for Use of Military Force (“AUMF”), a joint resolution authorizing the President “to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed or aided the terrorist attacks.”<sup>9</sup> War had begun, and the U.S. military soon invaded Afghanistan.

In November 2001, during clashes between American forces and the Taliban, an Afghan militia captured Salim Ahmed Hamdan and transferred him to U.S. custody.<sup>10</sup> In June 2002, the military brought him to the U.S. Naval Station in Guantánamo Bay, Cuba, where he was detained as an enemy combatant.<sup>11</sup> After Hamdan had spent more than a year in detention,

---

<sup>6</sup> Pub. L. No. 109-366, 120 Stat. 2600, 2630 (2006) (codified at 10 U.S.C. § 948a note). Congress enacted the 2009 MCA as part of its National Defense Authorization Act for Fiscal Year 2010. See Pub. L. No. 111-84, 123 Stat. 2574 (2009) (codified at 10 U.S.C. § 948a note); accord Exec. Order No. 13,492, 74 Fed. Reg. 4,897 (Jan. 22, 2009) (halting all proceedings under the 2006 MCA pending detainee review). Although the 2009 MCA replaced the 2006 MCA, many provisions remained the same. Cf. 123 Stat. at 2612 § 1804 (ratifying convictions under 2006 MCA). Given that the original Act was at issue in *Hamdan II* and the changes are not relevant to the case, this Article refers to the 2006 MCA unless otherwise noted.

<sup>7</sup> *Hamdan v. Gates*, 565 F. Supp. 2d 130, 137 (D.D.C. 2008).

<sup>8</sup> Military Order, *supra* note 2, § 1(a); cf. Jeh Johnson, General Counsel, U.S. Dep’t of Def., The Conflict Against Al Qaeda and Its Affiliates: How Will It End?, Oxford Union Address at Oxford University (Nov. 30, 2012) (proposing “a tipping point at which so many of the leaders and operatives of al Qaeda and its affiliates have been killed or captured” as the end of armed conflict).

<sup>9</sup> Pub. L. No. 107-40, 115 Stat. 224 (2001) (codified at 50 U.S.C. § 1541 note).

<sup>10</sup> *Hamdan I*, 548 U.S. at 566.

<sup>11</sup> *Id.*; *Hamdan II*, 696 F.3d at 1243; cf. Memorandum from Paul Wolfowitz, Deputy Secretary of Defense, to the Secretary of the Navy, Order Establishing Combatant Status Review Tribunal 1 (July 7, 2004), available at <http://www.defense.gov/news/Jul2004/d20040707review.pdf>. (defining “enemy combatant” as “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”).

President Bush declared that he was to be tried by military commission.<sup>12</sup> After another year in detention, Hamdan learned his charge: one count of conspiracy “to commit . . . offenses triable by military commission,” including attacking civilians, murder, and terrorism.<sup>13</sup>

Hamdan is a Yemeni national who had served as driver and bodyguard for Osama bin Laden from 1996 to 2001.<sup>14</sup> A member of the “international terrorist organization” al Qaeda,<sup>15</sup> he was alleged to have transported weapons and received weapons training in al Qaeda camps.<sup>16</sup> Facing trial by military commission for conspiracy, Hamdan filed petitions for writs of habeas corpus and mandamus to challenge the legality of the proceedings.<sup>17</sup>

In 2006, the Supreme Court in *Hamdan I* ruled in his favor. The Bush Administration’s system of military commissions was sparse, to say the least, as the President had declared it “not practicable to apply in military commissions . . . the principles of law and the rules of evidence generally recognized in the trial of criminal cases in the United States district courts.”<sup>18</sup> For example, a detainee could be excluded from his own trial and convicted based on evidence he had never seen.<sup>19</sup> The Court held that this system of military commissions lacked congressional authorization and failed to adhere to both the Uniform Code of Military Justice and the Geneva Conventions.<sup>20</sup> Exigency lent legitimacy to a military commission, “but did not further justify the wholesale jettisoning of procedural protections.”<sup>21</sup> If the Executive wanted to try detainees by military commission, it would have to afford “at least the barest of those trial protections that have been recognized by customary international law.”<sup>22</sup> In a plurality opinion, four justices also decided that conspiracy was not an offense against the law of war and, so, not triable by military commission.<sup>23</sup>

---

<sup>12</sup> *Hamdan I*, 548 U.S. at 566.

<sup>13</sup> Charge: Conspiracy, *United States v. Hamdan*, available at <http://www.defense.gov/news/Jul2004/d20040714hcc.pdf>; see *Hamdan I*, 548 U.S. at 566; *United States v. Hamdan*, 801 F. Supp. 2d 1247, 1259 (C.M.C.R. 2011) (en banc), *rev’d*, 696 F.3d 1238 (D.C. Cir. 2012). Hamdan was formally charged on July 13, 2004, after two years and eight months in detention. See *Hamdan*, 565 F. Supp. 2d at 131.

<sup>14</sup> See *Hamdan I*, 548 U.S. at 570; *Hamdan II*, 696 F.3d at 1242.

<sup>15</sup> *Hamdan II*, 696 F.3d at 1240.

<sup>16</sup> See *Hamdan I*, 548 U.S. at 570; *Hamdan II*, 696 F.3d at 1242.

<sup>17</sup> *Hamdan I*, 548 U.S. at 567.

<sup>18</sup> Military Order, *supra* note 2, § 1(f).

<sup>19</sup> *Hamdan I*, 548 U.S. at 614-16.

<sup>20</sup> *Id.* at 567, 594-95, 624-25, 635.

<sup>21</sup> *Id.* at 624.

<sup>22</sup> *Id.* at 633.

<sup>23</sup> Compare *id.* at 603-04, 611 (Stevens, J., plurality) (“The crime of ‘conspiracy’ has rarely if ever been tried as such in this country by any law-of-war military commission not exercising

Within four months after the Supreme Court's opinion in *Hamdan I*, Congress responded by enacting the Military Commissions Act of 2006.<sup>24</sup> The MCA restyled the military commissions system by codifying procedural safeguards for defendants.<sup>25</sup> It also enumerated twenty-eight specific offenses as "triable by military commission . . . at any time without limitation."<sup>26</sup> Among these offenses, the MCA allowed punishment by military commission for anyone who "conspires to commit" substantive offenses and for anyone who knowingly or intentionally provides "material support or resources" for terrorism.<sup>27</sup> The Act defined "material support or resources" broadly to mean "any property, tangible or intangible, or service."<sup>28</sup>

With the MCA in hand and a more robust trial structure in place, the government prosecuted Hamdan anew—and added a charge of material support for terrorism to the original charge of conspiracy.<sup>29</sup> Just as he did

---

some other form of jurisdiction, and does not appear in either the Geneva Conventions or the Hague Conventions—the major treaties on the law of war.") *with id.* at 698–703 (Thomas, J., dissenting) ("[T]he experience of our wars is rife with evidence that establishes beyond any doubt that conspiracy to violate the laws of war is itself an offense cognizable before a law-of-war military commission.") (internal quotations omitted).

<sup>24</sup> See *Hamdan II*, 696 F.3d at 1243–44. The Supreme Court decided *Hamdan I* on June 29, 2006, and Congress passed the MCA on October 17, 2006.

<sup>25</sup> See, e.g., 10 U.S.C. §§ 948k (effective assistance of counsel), 948r (no compulsory self-incrimination nor admission of statements obtained by torture), 948s (access to charges in defendant's native language and "sufficiently in advance of trial"), 949a(b)(1)(B) (right to be present at trial), 949c(b)(7) (right to cross-examine witnesses), 949l (presumption of innocence); *accord Hamdan*, 565 F. Supp. 2d at 132 (comparing structure of military commissions to courts-martial and federal trials). The 2009 MCA went further by prohibiting "the use of statements obtained by cruel, inhuman and degrading treatment—what was once the most controversial aspect of military commissions." Jeh Johnson, National Security Law, Lawyers and Lawyering in the Obama Administration, Speech at Yale Law School (Feb. 22, 2012); see 10 U.S.C.

§ 948r (2009).

<sup>26</sup> 10 U.S.C. § 950v(b).

<sup>27</sup> *Id.* § 950v(b)(25), (28). Congress included the same proscription of material support for terrorism in the 2009 MCA, over the objection of the Obama Administration. See 10 U.S.C. § 950t(25) (2009); *Military Commissions: Hearing to Receive Testimony on Legal Issues Regarding Military Commissions and the Trial of Detainees for Violations of the Law of War Before the S. Comm. on Armed Services*, 111th Cong. 1 (2009) ("[T]here is a significant risk that appellate courts will ultimately conclude that material support for terrorism is not a traditional law of war offense, thereby reversing hard-won convictions and leading to questions about the system's legitimacy.") (statement of Assistant Attorney General David Kris).

<sup>28</sup> 10 U.S.C. § 950v(b)(25)(B) (incorporating definition of "material support or resources" from 18 U.S.C. § 2339A(b)).

<sup>29</sup> See *Hamdan II*, 696 F.3d at 1243–44; see also Charge Sheet for Salim Ahmed Hamdan (April 5, 2007), [http://www.mc.mil/Portals/0/pdfs/Hamdan%20\(AE001\).pdf](http://www.mc.mil/Portals/0/pdfs/Hamdan%20(AE001).pdf). The later prosecution of Hamdan did not constitute double jeopardy because, under the MCA, jeopardy attaches only

when facing his first military commission, Hamdan sought to stop the proceedings as unlawful.<sup>30</sup> He filed a petition for habeas corpus and a motion for preliminary injunction in the U.S. District Court for the District of Columbia, seeking relief from the same judge who had granted his prior habeas petition.<sup>31</sup> This time around, the district court refused Hamdan's requests in light of "enactment of the MCA."<sup>32</sup> Absent federal court intervention, Hamdan was tried by military commission in Guantánamo and received a mixed verdict. He was acquitted of conspiracy but convicted of two types of providing material support for terrorism: providing "material support for carrying out an act of terrorism" and providing "material support to an international terrorist organization."<sup>33</sup>

In August 2008, Hamdan was sentenced to a prison term of sixty-six months.<sup>34</sup> With credit for his many years detained in Guantánamo, he served only a few more months in prison.<sup>35</sup> In November 2008, the military transferred Hamdan to his native Yemen to serve the remaining weeks of his sentence, and in January 2009 Yemeni authorities released him.<sup>36</sup> Even after release, Hamdan continued to appeal his conviction.<sup>37</sup>

As a first appellate step, the U.S. Court of Military Commission Review affirmed the trial court's finding and sentence.<sup>38</sup> Hamdan then appealed as of right to the U.S. Court of Appeals for the D.C. Circuit, which holds "exclusive jurisdiction to determine the validity of a final judgment rendered by a military commission."<sup>39</sup> In October 2012, the civilian appellate court reversed and

---

when a "finding of guilty has become final after review of the case has been fully completed." 10 U.S.C. § 949h. Far from yielding a completed review of a guilty finding, Hamdan's prior litigation effectively shut down the military commissions system through his habeas and mandamus petitions.

<sup>30</sup> See *Hamdan*, 565 F. Supp. 2d at 131; *Hamdan v. Rumsfeld*, 464 F. Supp. 2d 9, 10 (D.D.C. 2006); *Hamdan v. Rumsfeld*, 344 F. Supp. 2d 152, 155 (D.D.C. 2004), *rev'd*, 415 F.3d 33 (D.C. Cir. 2005), *rev'd*, 548 U.S. 557 (2006).

<sup>31</sup> See *Hamdan*, 344 F. Supp. 2d at 173 (granting pre-MCA habeas petition).

<sup>32</sup> *Hamdan*, 565 F. Supp. 2d at 136 (denying post-MCA motion for preliminary injunction); see *Hamdan*, 464 F. Supp. 2d at 19 (denying post-MCA habeas petition), *rev'd sub nom.*, *Boumediene v. Bush*, 553 U.S. 723 (2008).

<sup>33</sup> *Hamdan*, 801 F. Supp. 2d at 1258-59; see *Hamdan II*, 696 F.3d at 1244. Hamdan's charge of providing material support for terrorism contained eight specifications; he was convicted of five of those specifications. See 696 F.3d at 1244.

<sup>34</sup> *Hamdan II*, 696 F.3d at 1244.

<sup>35</sup> *Id.* at 1241, 1244.

<sup>36</sup> *Id.* at 1244; *Hamdan*, 801 F. Supp. 2d at 1260.

<sup>37</sup> *Hamdan II*, 696 F.3d at 1244. The court held that Hamdan's completed sentence and release did not render his appeal moot. See *id.* at 1244-45.

<sup>38</sup> *Hamdan*, 801 F. Supp. 2d at 1254.

<sup>39</sup> 10 U.S.C. § 950g(a); see 10 U.S.C. § 950g(a) (2009).



vacated the conviction.<sup>40</sup>

The D.C. Circuit Court accepted the Executive Branch's view that the United States is at war against the terrorist organization al Qaeda.<sup>41</sup> From that starting point, the court reviewed Hamdan's conviction with an eye toward achieving Congress' intent stated in the MCA and avoiding an Ex Post Facto Clause violation.<sup>42</sup> Congress intended the MCA to "codify offenses that have traditionally been triable by military commissions" and not to "establish new crimes."<sup>43</sup> As merely "declarative of existing law," the Act allowed prosecution of crimes that occurred before enactment.<sup>44</sup> On the court's interpretation, however, the MCA did "codify some new war crimes, including material support for terrorism."<sup>45</sup> Consistent with Congress' intent and the Constitution's ex post facto prohibition, the MCA could not authorize retroactive prosecution for these new crimes.<sup>46</sup> Given that the Act passed in 2006, its proscription of material support for terrorism could not apply to Hamdan's alleged activities supporting bin Laden and al Qaeda between 1996 and 2001.<sup>47</sup> Accordingly, he could be convicted only if a prior law criminalized material support for terrorism.<sup>48</sup>

The court examined the relevant law at the time of Hamdan's alleged misconduct and found it wanting.<sup>49</sup> Specifically, Section 821 of U.S. Code Title 10 provides "jurisdiction with respect to offenders or offenses that by statute or by the law of war may be tried by military commissions."<sup>50</sup> Two longstanding statutory offenses called for military commissions: spying in time of war and aiding the enemy.<sup>51</sup> Neither was at issue for Hamdan. So the court focused on "law of war" offenses and interpreted that language by reference to international law.<sup>52</sup> Certain forms of terrorism, including targeting civilians and aiding and abetting terrorist acts, are long recognized as international-law

---

<sup>40</sup> *Hamdan II*, 696 F.3d at 1241.

<sup>41</sup> *See id.* at 1240.

<sup>42</sup> *See id.* at 1241, 1247–48; U.S. CONST. art. I, § 9, cl. 3 ("No bill of attainder or ex post facto Law shall be passed.").

<sup>43</sup> 10 U.S.C. § 950p(a). Congress restated this intent in the 2009 MCA. *See* 10 U.S.C. § 950p(d) (2009) ("This chapter does not establish new crimes . . .").

<sup>44</sup> 10 U.S.C. § 950p(b).

<sup>45</sup> *Hamdan II*, 696 F.3d at 1247.

<sup>46</sup> *See id.* at 1247–48 ("Congress would *not* have wanted *new* crimes to be applied retroactively.") (emphasis in original).

<sup>47</sup> *Id.* at 1248.

<sup>48</sup> *Id.*

<sup>49</sup> *Id.* at 1248–51.

<sup>50</sup> 10 U.S.C. § 821.

<sup>51</sup> *See id.* §§ 904, 906

<sup>52</sup> 696 F.3d at 1248–51 (citing *Hamdan I*, 548 U.S. at 603, 610, 641).

war crimes.<sup>53</sup> Not so for material support for terrorism.<sup>54</sup> Observing that even the Executive Branch acknowledged that material support for terrorism was not a war crime under international law, the court concluded that there was no timely proscription of that offense.<sup>55</sup> Hamdan's conviction could not stand.<sup>56</sup> Essentially, the conviction collapsed under the statute's internal ex post facto tension: punishment for prior commission of a new crime, specified by an Act that did not authorize retroactive punishment for new crimes.<sup>57</sup>

The outcome in *Hamdan II* borders on the self-referential, bringing the defendant's involvement in the post-9/11 world full circle. Hamdan was convicted of a crime specified in the MCA, a law that Congress passed in direct response to the Supreme Court's opinion in *Hamdan I*. Thus, the law that codified the new crime of material support for terrorism, which became a charge against Hamdan in his second foray into the military commissions system, came into being only because Hamdan had challenged his first foray into the military commissions system. And that law's untimely passage was the basis for the appellate court's vacatur of Hamdan's conviction.<sup>58</sup>

In the end, after years of litigation and more than a decade after the September 11th attacks, Hamdan is home and his name is clear.

### III. THE IMPACT OF *HAMDAN II* ON MILITARY COMMISSIONS

During Congressional debates on the 2009 revisions to the MCA, the Obama Administration expressed concern that reversals of convictions for material support for terrorism would "lead[] to questions about the system's legitimacy."<sup>59</sup> Those questions rose quickly and loudly in the media after

---

<sup>53</sup> *Id.* at 1250–51.

<sup>54</sup> *Id.* at 1250.

<sup>55</sup> *Id.* at 1251–52.

<sup>56</sup> *Id.* at 1253.

<sup>57</sup> Following the doctrine of constitutional avoidance, the court declined to decide the "ultimate constitutional question" of whether the Ex Post Facto Clause applied to Hamdan's conviction. *Id.* at 1248 & n. 7.

<sup>58</sup> The same constitutional clause that prohibits ex post facto laws also prohibits bills of attainder. See U.S. CONST. art. I § 9, cl. 3. A bill of attainder is a "special legislative act prescribing punishment, without a trial, for a specific person or group." BLACK'S LAW DICTIONARY 188 (9th ed. 2009). While the MCA did not name anyone, Congress undoubtedly had Hamdan and other Guantánamo detainees in mind when passing the MCA immediately after *Hamdan I*. See *Boumediene v. Bush*, 476 F.3d 981, 986 (D.C. Cir. 2007) ("Everyone who has followed the interaction between Congress and the Supreme Court knows full well that one of the primary purposes of the MCA was to overrule *Hamdan*."), *rev'd*, 553 U.S. 723 (2008). Nonetheless, the military judge overseeing Hamdan's trial considered and rejected his constitutional challenge based on bill of attainder. See *Hamdan*, 565 F. Supp. 2d at 133.

<sup>59</sup> *Military Commissions: Hearing to Receive Testimony on Legal Issues Regarding Military Commissions and the Trial of Detainees for Violations of the Law of War Before the S. Comm.*

*Hamdan II*. The opinion was portrayed as “strik[ing] a powerful blow to the legitimacy” of the terrorism trials in Guantánamo.<sup>60</sup> Some commentators raised the volume on their terminology: this “blockbuster opinion”<sup>61</sup> from a conservative circuit struck “the biggest blow yet against the legitimacy of the Guantánamo military commissions”<sup>62</sup> and served to rein in “executive branch officials [who] stubbornly sought to manipulate the rule of law.”<sup>63</sup>

Guantánamo is a sensitive topic. *Hamdan II* bears close and measured scrutiny as a recent addition to federal courts’ detainee jurisprudence. Contrary to its media depiction, the D.C. Circuit Court’s opinion poses no existential threat to Guantánamo military commissions. Quite the opposite: the opinion is good authority to convene future military commissions. While formal convening authority rests with the Secretary of Defense, courts offer the complementary authority of judicial review.<sup>64</sup> *Hamdan I* recognized exigency as lending legitimacy to military commissions.<sup>65</sup> Six years later, *Hamdan II* recognized the trial process as lending further legitimacy. The D.C. Circuit Court accepted that the United States is at war, upheld the structure of military commissions, and guided prosecutors to charge defendants carefully for conduct before or after enactment of the MCA. Upon examination, the opinion is a typical appellate disapproval of a trial result—based not on the illegitimacy of the proceedings but on the misapplication of a new law.

Just as appellate courts do every day, the D.C. Circuit Court in *Hamdan II* reviewed a lower-court criminal proceeding and found a flaw. This was a fatal flaw, to be sure, as all governmental branches agreed that the MCA should not be construed to violate the Constitution’s Ex Post Facto Clause.<sup>66</sup> That clause embodies a basic and ancient notion of fairness in our jurisprudence:

---

on Armed Services, 111th Cong. 1 (2009) (statement of Assistant Attorney General David Kris).

<sup>60</sup> Andy Worthington, *Conservative Judges Demolish the False Legitimacy of Guantánamo’s Terror Trials*, EURASIA REV., Nov. 11, 2012, <http://www.eurasiareview.com/11112012-conservative-judges-demolish-the-false-legitimacy-of-guantanamos-terror-trials-oped/>.

<sup>61</sup> Kevin Jon Heller, *D.C. Circuit: Material Support for Terrorism Not a War Crime (Prior to 2001)*, OPINION JURIS, Oct. 16, 2012, <http://opiniojuris.org/2012/10/16/d-c-circuit-material-support-for-terrorism-not-a-war-crime-prior-to-2001/>.

<sup>62</sup> John H. Cushman, Jr., *Appeals Court Overturns Terrorism Conviction of Bin Laden’s Driver*, N.Y. TIMES, Oct. 16, 2012, [http://www.nytimes.com/2012/10/17/us/politics/appeals-court-overturns-terrorism-conviction-of-salim-ahmed-hamdan-bin-ladens-driver.html?\\_r=0](http://www.nytimes.com/2012/10/17/us/politics/appeals-court-overturns-terrorism-conviction-of-salim-ahmed-hamdan-bin-ladens-driver.html?_r=0) (quoting ACLU attorney Zachary Katznelson).

<sup>63</sup> Andrew Cohen, *This Month in Terror Law: Salim Hamdan Wins Again!*, THE ATLANTIC, Oct. 16, 2012, <http://www.theatlantic.com/national/archive/2012/10/this-month-in-terror-law-salim-hamdan-wins-again/263692/>.

<sup>64</sup> See 10 U.S.C. § 948h (2009); cf. *Boumediene*, 553 U.S. at 738 (respecting the “ongoing dialogue between and among the branches of Government” with respect to the MCA).

<sup>65</sup> 548 U.S. at 624.

<sup>66</sup> See *Hamdan II*, 696 F.3d at 1247–48.

"individuals should have an opportunity to know what the law is and to conform their conduct accordingly."<sup>67</sup> But the panel struck no blow to the legitimacy of the whole proceeding. Immediately upon directing that "Hamdan's conviction for material support for terrorism be vacated," the court wrote a significant clarification: its opinion does *not* "preclude any future military commission charges against Hamdan—either for conduct prohibited by the 'law of war' under 10 U.S.C. § 821 or for any conduct since 2006 that has violated the Military Commissions Act."<sup>68</sup> The opinion rejected Hamdan's conviction on a reasoned basis, but not the process that generated that conviction. The court offered a straightforward timeliness analysis and took pains to spell out that it offered nothing more. Indeed, the D.C. Circuit Court's many rulings in *ex post facto* cases underscore the importance of a timely prohibition.<sup>69</sup>

Thus, *Hamdan II* invites future trials by military commission and provides an appellate-sanctioned roadmap for the proceedings. Should the Executive seek to try an individual by military commission for actions that were criminalized before he undertook them, it may do so—just as it may do so in the ordinary course in Article III courts. For conduct before 2006, international-law war crimes have long included terrorism, aiding and abetting terrorism, and targeting civilians.<sup>70</sup> Additionally, many decades ago Congress codified spying

---

<sup>67</sup> *Landgraf v. USI Film Prods.*, 511 U.S. 244, 265 (1994) (finding damages and jury trial provisions not retroactive); see *Kaiser Aluminum & Chem. Corp. v. Bonjorno*, 494 U.S. 827, 855 (1990) (Scalia, J., concurring) ("principle that the legal effect of conduct should ordinarily be assessed under the law that existed when the conduct took place has timeless and universal appeal"); *Dash v. Van Kleeck*, 7 Johns. 477, 503 (N.Y. 1811) ("It is a principle of the English common law, as ancient as the law itself, that a statute, even of its omnipotent parliament, is not to have a retrospective effect.") (Kent, C.J.). As far back as *The Federalist Papers*, Alexander Hamilton condemned the "creation of crimes after the commission of the fact" as one of "the favorite and most formidable instruments of tyranny." THE FEDERALIST NO. 84 (Alexander Hamilton).

<sup>68</sup> *Hamdan II*, 696 F.3d at 1241 & n.1.

<sup>69</sup> See, e.g., *Fletcher v. Reilly*, 433 F.3d 867, 879 (D.C. Cir. 2006) (finding *prima facie* case that defendant's "rights under the Ex Post Facto Clause have been violated, because he is a D.C. Code offender whose parole was revoked based on an offense that was not a D.C. Code offense"); *United States v. Rezaq*, 134 F.3d 1121, 1141 n.13 (D.C. Cir. 1998) (declining to apply recently amended restitution statute because "the Ex Post Facto Clause prohibits the application of this amendment" to defendant); *United States v. Booze*, 108 F.3d 378, 381 n.3 (D.C. Cir. 1997) (considering proper sentence for drug offender and noting that "resentencing occurs under the version of the Guidelines in effect at the time of resentencing, unless such an application would violate the Ex Post Facto Clause"); *United States v. Lam Kwong-Wah*, 924 F.2d 298, 304 (D.C. Cir. 1991) (vacating sentence for conspiracy and remanding because, where later sentencing guidelines would "adversely affect" defendant's sentence, they "may not be applied retroactively without violating the *ex post facto* clause").

<sup>70</sup> See *Hamdan II*, 696 F.3d at 1250–51.

and aiding the enemy as war crimes, on penalty of death.<sup>71</sup> For conduct after 2006, the MCA specifies a myriad of crimes including material support for terrorism.

*Hamdan II* clarifies the military commissions procedure, and that clarity is legitimating. Given the D.C. Circuit Court's exclusive jurisdiction to review military commission judgments,<sup>72</sup> there is neither an opportunity for forum shopping nor a chance of a circuit split. On military commission matters, the D.C. Circuit answers only to itself and the Supreme Court.<sup>73</sup> But clarity should not be mistaken for simplicity. Any MCA charges of "new war crimes,"<sup>74</sup> including material support for terrorism, are vulnerable under *Hamdan II*'s timeliness analysis. While Guantánamo holds al Qaeda leaders directly involved in terrorist plots against the United States, many of the current 166 detainees are "low-level foreign fighters" who lacked a significant role in terrorist organizations.<sup>75</sup> Seven detainees have military commission charges pending.<sup>76</sup> The task of swearing and proving charges remains difficult, and the stakes for both prosecutors and defendants remain high.

The stakes are particularly high in the military commission trial underway in Guantánamo against "those we believe were responsible for the 9/11 attacks," most notably Khalid Shaikh Mohammad.<sup>77</sup> Mohammad is a "high-value" detainee who has proclaimed himself a "jackal" and the "mastermind" behind the September 11th attacks.<sup>78</sup> He and four co-defendants<sup>79</sup> are charged under

<sup>71</sup> See 10 U.S.C. §§ 904, 906. Both offenses are also included in the MCA. See 10 U.S.C. § 950v(26), (27); 10 U.S.C. § 950t(26), (27) (2009).

<sup>72</sup> See 10 U.S.C. § 950g(a).

<sup>73</sup> See *id.* § 950g(e) ("The Supreme Court may review by writ of certiorari pursuant to section 1254 of title 28 the final judgment of the United States Court of Appeals for the District of Columbia Circuit under this section."); see also *Hamdan v. Gates*, 565 F. Supp. 2d 130, 137 (D.D.C. 2008) ("If the Military Commission judge gets it wrong, his error may be corrected by the CMCR. If the CMCR gets it wrong, it may be corrected by the D.C. Circuit. And if the D.C. Circuit gets it wrong, the Supreme Court may grant a writ of certiorari.").

<sup>74</sup> *Hamdan II*, 696 F.3d at 1247.

<sup>75</sup> GUANTÁNAMO REVIEW TASK FORCE, FINAL REPORT 19 (2010). (describing categories of detainees); GAO REPORT, *supra* note 3, at 8–9 (166 detainees as of November 2012).

<sup>76</sup> GAO REPORT, *supra* note 3, at 8–9.

<sup>77</sup> Press Release, Dep't of Justice, Departments of Justice and Defense Announce Forum Decisions for Ten Guantánamo Bay Detainees (Nov. 13, 2009), *available at* <http://www.justice.gov/opa/pr/2009/November/09-ag-1224.html> (statement of Attorney General Eric H. Holder, Jr.). Attorney General Holder initially planned to try the 9/11 defendants in the U.S. District Court for the Southern District of New York. *Id.*

<sup>78</sup> See GAO REPORT, *supra* note 3, at 15, 31; *Khalid Shaikh Mohammed (Guantánamo 9/11 Attacks Trial)*, N.Y. TIMES, Oct. 18, 2012, [http://topics.nytimes.com/top/reference/timestopics/people/m/khalid\\_shaikh\\_mohammed/index.html](http://topics.nytimes.com/top/reference/timestopics/people/m/khalid_shaikh_mohammed/index.html).

<sup>79</sup> The co-defendants are Walid Muhammad Salih Mubarak Bin 'Attash, Ramzi Binalshibh, Ali

the 2009 MCA with eight offenses: "conspiracy, murder in violation of the law of war, attacking civilians, attacking civilian objects, intentionally causing serious bodily injury, destruction of property in violation of the law of war, hijacking aircraft, and terrorism."<sup>80</sup>

The September 11th defendants do not face charges of material support for terrorism.<sup>81</sup> *Hamdan II* nonetheless weakens the MCA charge of conspiracy, especially given the Supreme Court's plurality opinion in *Hamdan I* that rejected conspiracy as a war crime.<sup>82</sup> Even the chief prosecutor has assessed the conspiracy charge to fail under the D.C. Circuit Court's analysis.<sup>83</sup> And the government chose not to oppose defendants' motion to dismiss conspiracy as a separate and standalone offense, on the basis that dismissal would "avoid introducing additional uncertainty and appellate risk into this capital case" and allow the case "to proceed without unnecessary delay."<sup>84</sup>

---

Abdul Aziz Ali, and Mustafa Ahmed Adam al Hawsawi. See Brigadier General Mark Martins, Chief Prosecutor, Memorandum Thru Legal Advisor to the Convening Authority (Jan. 6, 2013) at 2. The government dropped charges against another detainee, Mohammed al Qahtani, because he had been tortured during interrogations. See Bob Woodward, *Guantánamo Detainee Was Tortured, Says Official Overseeing Military Trials*, WASH. POST, Jan. 14, 2009, <http://www.washingtonpost.com/wpdyn/content/article/2009/01/13/AR2009011303372.html>.

<sup>80</sup> Press Release, Dep't of Defense, DOD Announces Charges Sworn Against Five Detainees Allegedly Responsible for 9/11 Attacks (May 31, 2011), available at <http://www.defense.gov/releases/release.aspx?releaseid=14532>; see Charge Sheet of Khalid Shaikh Mohammad, United States v. Khalid Shaikh Mohammad (May 31, 2011), available at <http://www.mc.mil/CASES/MilitaryCommissions.aspx>.

<sup>81</sup> Previous charges included material support to terrorism. See Dep't of Defense News Transcript, *DoD News Briefing with Brig. Gen. Hartmann from the Pentagon* (Feb. 11, 2008), <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4142>.

<sup>82</sup> See 548 U.S. at 603–04.

<sup>83</sup> See Brigadier General Mark Martins, Chief Prosecutor, Memorandum Thru Legal Advisor to the Convening Authority (Jan. 6, 2013) at 2. The convening authority for the military commission, retired Vice Admiral Bruce MacDonald, informed Brigadier General Martins that it would be "premature to withdraw and dismiss the conspiracy charge." Dep't of Defense News Release No. 029-13, *Convening Authority for Military Commissions Declines to Withdraw Conspiracy Charge Against Alleged 9/11 Co-Conspirators Pending Appellate Ruling* (Jan. 18, 2013), <http://www.defense.gov/releases/release.aspx?releaseid=15779>.

<sup>84</sup> Brigadier General Mark Martins, Chief Prosecutor, Remarks at Guantánamo Bay (Jan. 27, 2013) (adding condition that "the Commission agrees to approve minor conforming changes to the charge sheet" to "preserve the existing co-conspirator theory of liability"); see Charlie Savage, *U.S. To Press Fight of Detainee's Appeal*, N.Y. TIMES, Jan. 9, 2013, at A14 (quoting Brigadier General Martins' recommendation to drop conspiracy charges in order to "remove an issue that could otherwise generate uncertainty and delay"). As is plain from the disagreement between plurality and dissenting opinions in *Hamdan I*, the issue of whether conspiracy is a war crime is not new. See 548 U.S. at 603–04, 611, 698–703. Although *Hamdan* was acquitted of conspiracy in *Hamdan II*, this issue is squarely presented in another Guantánamo detainee case appealed from the Court of Military Commission Review to the D.C. Circuit Court. See

Dropping the conspiracy charge against the September 11th defendants would reduce the number of charges from eight to seven. It would not end the case. Applying the strictest reading of *Hamdan II* and including only offenses that were “firmly grounded” international-law war crimes before Congress passed the MCA,<sup>85</sup> serious charges remain. Attacking civilians and terrorism are established offenses against the law of war,<sup>86</sup> and those charges suffice to try Mohammad and his co-defendants by military commission.<sup>87</sup>

The logic of *Hamdan II* also applies to prior convictions obtained by military commission in Guantánamo: to the extent convictions for pre-2006 conduct were based on offenses recognized as war crimes, those convictions should stand. Seven Guantánamo detainees have been convicted through military commissions; four were subsequently transferred to other countries.<sup>88</sup> In addition to Hamdan, one other detainee was convicted solely of providing material support for terrorism.<sup>89</sup> Australian citizen David Hicks pleaded guilty in 2007 to one count of providing material support for terrorism.<sup>90</sup> He was

---

United States v. Al Bahlul, 820 F. Supp. 2d 1141 (C.M.C.R. 2011) (en banc) (affirming convictions for conspiracy, material support for terrorism, and solicitation), *rev'd*, No. 11–1324, 2013 WL 297726, at \*1 (D.C. Cir. Jan. 25, 2013). There, the government filed a brief advising the D.C. Circuit Court that “*Hamdan II* requires reversal of Bahlul’s convictions by military commission,” but preserving its arguments for further review. Supplemental Brief for United States at 1, *Al Bahlul v. United States*, No. 11–1324 (D.C. Cir. Jan. 9, 2013) (No. 1414342), 2013 WL 122618, at \*1; *see Al Bahlul*, 2013 WL 297726, at \*1 (vacating convictions). Attorney General Holder is pressing forward with the *Bahlul* case despite recommendations otherwise. *See* Charlie Savage, *U.S. To Press Fight of Detainee’s Appeal*, N.Y. TIMES, Jan. 9, 2013, at A14.

<sup>85</sup> *Hamdan II*, 696 F.3d at 1250 n.10.

<sup>86</sup> *See id.* at 1249–50 (“It is true that international law establishes at least some forms of terrorism, including the intentional targeting of civilian populations, as war crimes.”) (emphasis in original).

<sup>87</sup> Jane Sutton, *Guantánamo Prosecutor Wants Conspiracy Charge Dropped in 9/11 Case*, NBCNEWS.COM (Jan. 10, 2013), [http://usnews.nbcnews.com/\\_news/2013/01/10/16442972-guantanamo-prosecutor-wants-conspiracy-charge-dropped-in-911-case?lite](http://usnews.nbcnews.com/_news/2013/01/10/16442972-guantanamo-prosecutor-wants-conspiracy-charge-dropped-in-911-case?lite) (quoting Brigadier General Martins that “[t]here is a clear path forward for legally sustainable charges”).

<sup>88</sup> GAO REPORT, *supra* note 3, at 8–9 & n.17; *see also The Guantánamo Trials*, HUM. RTS. WATCH, <http://www.hrw.org/features/Guantanamo> (last visited Mar. 28, 2013). One detainee, Ahmed Khalfan Ghailani, was transferred from Guantánamo to federal court in the Southern District of New York, where he was convicted of conspiracy. *See* GAO REPORT, *supra* note 3, at 11; Human Rights Watch, *Ahmed Khalfan Ghailani* (2012), <http://www.hrw.org/news/2012/10/25/ahmed-khalfan-ghailani>.

<sup>89</sup> *See Military Commissions Cases*, MILITARY COMMISSIONS, <http://www.mc.mil/CASES/MilitaryCommissions.aspx> (last visited Mar. 28, 2013); *The Guantánamo Trials*, HUM. RTS. WATCH, <http://www.hrw.org/features/Guantanamo> (last visited Mar. 28, 2013); *Names of the Detained in Guantánamo Bay*, WASH. POST (Dec. 20, 2012), <http://projects.washingtonpost.com/guantanamo/>.

<sup>90</sup> *See* Dep’t of Defense News Release No. 362–07, *Detainee Convicted of Terrorism Charge at Guantánamo Trial* (Mar. 30, 2007), <http://www.defense.gov/releases/release.aspx>.

sentenced to seven years, which by plea agreement was reduced to nine months' confinement in Australia.<sup>91</sup> He was released on December 29, 2007.<sup>92</sup> As part of his plea agreement, Hicks waived all appeals.<sup>93</sup> Given this waiver, *Hamdan II* undercuts Hicks' conviction in theory if not in practice.<sup>94</sup>

#### IV. REACH OF *HAMDAN II* BEYOND MILITARY COMMISSIONS

Finally, the reach of *Hamdan II* extends beyond military commissions to Article III courts hearing terrorism cases. In addition to providing guidance on material support for terrorism under the MCA, the opinion suggests a fresh look at the related concepts of substantial support and direct support for terrorism. These concepts are at issue in *Hedges v. Obama*,<sup>95</sup> a case decided by the U.S. District Court for the Southern District of New York one month before *Hamdan II* and now on appeal to the U.S. Court of Appeals for the Second Circuit.

In *Hedges*, a group of journalists and activists filed suit to enjoin enforcement of Section 1021(b)(2) of the National Defense Authorization Act ("NDAA") for Fiscal Year 2012, which was enacted as an "affirmation" of executive detention authority under the Authorization for Use of Military Force of 2001.<sup>96</sup> Section 1021(b)(2) permits detention of any "person who was a part of or substantially supported al-Qaeda, the Taliban, or associated forces that are engaged in hostilities against the United States . . . or has directly supported such hostilities in aid of such enemy forces."<sup>97</sup> Plaintiffs challenged this

<sup>91</sup> See *id.*

<sup>92</sup> See *The Guantánamo Trials*, HUM. RTS. WATCH, <http://www.hrw.org/features/Guantánamo> (last visited Mar. 28, 2013). Hicks later published a book recounting his time in Guantánamo. See DAVID HICKS, *GUANTÁNAMO: MY JOURNEY* (2010).

<sup>93</sup> See Waiver of Appellate Review, *United States v. Hicks* (Mar. 30, 1997), <http://www.mc.mil/CASES/MilitaryCommissions.aspx>; Military Judge Markup of Pretrial Agreement, *United States v. Hicks* (Mar. 30, 1997), <http://www.mc.mil/CASES/MilitaryCommissions.aspx>.

<sup>94</sup> Two Guantánamo detainees were convicted by military commissions of only conspiracy and providing material support for terrorism. See *The Guantánamo Trials*, HUM. RTS. WATCH, <http://www.hrw.org/features/Guantánamo> (last visited Mar. 28, 2013). If the ultimate outcome in *Bahlul* is a rejection of conspiracy as a pre-2006 war crime, see *supra* note 84, then those convictions are similarly undercut.

<sup>95</sup> No. 12 Civ. 331 (KBF), 2012 WL 3999839, at \*1 (S.D.N.Y. Sept. 12, 2012).

<sup>96</sup> Pub. L. No. 112-81, 125 Stat. 1298, 1562 (2011) (codified at 10 U.S.C. § 801 note); see *id.* at 1562 §§ 1021(a) (Congress "affirms" presidential authority), (d) (not "limit or expand" AUMF), (e) (not "affect existing law or authorities"); AUMF, *supra* note 9; *Hedges*, 2012 WL 3999839, at \*\*6-13.

<sup>97</sup> 125 Stat. at 1562 § 1021(b)(2); see Johnson, *supra* note 25 (Obama Administration has interpreted AUMF to include "those persons who were part of, or substantially supported, Taliban or al-Qaeda forces or associated forces") (quoting Respondent's Memorandum Regarding the Government's Detention Authority Relative to Detainees Held at Guantánamo Bay at 2, *In re: Guantánamo Bay Detainee Litig.*, Misc. No. 08-442 (TFH) (D.D.C. Mar. 13, 2009)).



language as impermissibly vague under the Due Process Clause of the Fifth Amendment.<sup>98</sup> Due process requires, at minimum, “fair notice of what is prohibited.”<sup>99</sup> Although Section 1021(b)(2) is directed to terrorism, the language of “substantially supported,” “directly supported,” and “associated forces” is so vague that it puts even American citizens in the United States at risk of indefinite detention simply for reporting on terrorist organizations.<sup>100</sup> For example, the law might cover a news article that describes enemy forces favorably or American forces unfavorably.<sup>101</sup> The district court agreed, finding that “specificity is absent from Section 1021(b)(2)” and permanently enjoining enforcement.<sup>102</sup>

The government appealed, and in October 2012 the Second Circuit Court stayed the district court’s injunction pending a decision on the merits.<sup>103</sup> Two months later, plaintiffs filed an emergency application in the Supreme Court directed to Justice Scalia, asking the Court to vacate the Second Circuit’s stay.<sup>104</sup> The Court ultimately denied that application.<sup>105</sup> While plaintiffs’ appeal remains before the Second Circuit,<sup>106</sup> Congress has enacted the NDAA for Fiscal Year 2013.<sup>107</sup> This Act clarifies that nothing in the AUMF or the 2012 NDAA shall be construed to deny the writ of habeas corpus or constitutional rights in an Article III court to anyone in the United States who could otherwise invoke them.<sup>108</sup> The new language has not assuaged the *Hedges* plaintiffs’ concerns,

---

<sup>98</sup> See 2012 WL 3999839, at \*\*40–44; U.S. CONST. amend. V (“No person shall be . . . deprived of life, liberty, or property, without due process of law . . .”).

<sup>99</sup> *United States v. Williams*, 553 U.S. 285, 304 (2008) (“A conviction fails to comport with due process if the statute under which it is obtained fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standard less that it authorizes or encourages seriously discriminatory enforcement.”).

<sup>100</sup> 2012 WL 3999839, at \*\*40–44. The lead plaintiff, Christopher Hedges, is a Pulitzer Prize-winning foreign correspondent who engages with terrorists groups for his writing and journalism. See *id.* at \*\*6–8.

<sup>101</sup> *Id.* at \*\*33, 39.

<sup>102</sup> *Id.* at \*\*1–2, 40–45. The court had previously issued an order for a preliminary injunction. See *Hedges v. Obama*, No. 12 Civ. 331, 2012 WL 1721124, at \*1 (S.D.N.Y. May 16, 2012).

<sup>103</sup> See *Hedges v. Obama*, Nos. 12–3176 (L) & 12–3644(Con), 2012 WL 4075626, at \*1 (2d Cir. Sept. 17, 2012); Order Granting Stay, *Hedges v. Obama*, Nos. 12–3176 & 12–3644 (2d Cir. Oct. 2, 2012) (No. 78).

<sup>104</sup> See Plaintiffs-Petitioners’ Emergent Application to Vacate Temporary Stay of Permanent Injunction, *Hedges v. Obama* (Sup. Ct. Dec. 12, 2012).

<sup>105</sup> *Hedges v. Obama*, No. 12A600, 2013 WL 598441, at \*1 (Sup. Ct. Feb. 19, 2013).

<sup>106</sup> The Second Circuit Court heard oral argument on February 6, 2013. See Adam Klasfeld, *2nd Circuit Hearing on Indefinite Detention Focuses on Press Rights*, COURTHOUSE NEWS SERV., (Feb. 6, 2013), <http://www.courthousenews.com/2013/02/06/54640.htm>.

<sup>107</sup> Pub. L. No. 112-239, 126 Stat. 1632 (2013).

<sup>108</sup> *Id.* at 1917 § 1029 (codified at 10 U.S.C. § 801 note). This provision replaced an amendment to the 2013 NDAA introduced by Senators Dianne Feinstein and Mike Lee, which had been

and they continue to press their case.<sup>109</sup>

In evaluating the NDAA language of “substantial support” for terrorism, the district court heard echoes of the MCA language of “material support” for terrorism.<sup>110</sup> Consideration was fleeting, however, as the court agreed with the government-defendant that “the MCA plays no role in the case before this Court.”<sup>111</sup> The MCA may play no role in *Hedges* as a civilian case rather than a military case. But the NDAA is cast in a starring role, and *Hamdan II* offers a model for federal courts’ treatment of NDAA Section 1021.

The structure of the MCA’s proscription of material support for terrorism reflects the structure of the NDAA’s proscription of substantial or direct support for al Qaeda, the Taliban, or associated forces. That likeness suggests broader constitutional challenges. Congress enacted the MCA as legislation that “codifies crimes” but “does not establish new crimes.”<sup>112</sup> The D.C. Circuit Court in *Hamdan II* disagreed, finding that the MCA did establish new crimes and rejecting Hamdan’s retroactive punishment for the new crime of material support for terrorism.<sup>113</sup> By comparison, Congress enacted NDAA Section 1021 as legislation that “affirms” the President’s detention authority under the AUMF but does not “limit or expand that authority.”<sup>114</sup> The President agreed

---

drafted to “assure that no authorization to use military force, war declaration or any similar authority would allow an American apprehended in the United States to be held without charge or trial.” Press Release, Senator Feinstein, Senators Feinstein, Lee Introduce Amendment to Protect Civil Liberties (Nov. 28, 2012), *available at* <http://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=b5294991-c86f-4b13-8708-83db770d7740>; see Charlie Savage, *Congressional Negotiators Drop Ban on Indefinite Detention of Citizens*, *Aides Say*, N.Y. TIMES, Dec. 19, 2012, at A16.

<sup>109</sup> See Chris Hedges, *The Final Battle*, TRUTHDIG (Dec. 23, 2012), [http://www.truthdig.com/report/item/the\\_final\\_battle\\_20121223/](http://www.truthdig.com/report/item/the_final_battle_20121223/) (“[R]estoring due process for citizens was something the Republicans and the Democrats, along with the White House, refused to do.”); Michael Kelley, *Actually, The Newest Version Of NDAA Makes It EASIER To Detain Citizens Indefinitely*, BUS. INSIDER (Nov. 29, 2012), <http://www.businessinsider.com/ndaa-americans-indefinite-detention2012-11#ixzz2FVuWSold> (“The newest version of the NDAA seems to be equating the AUMF and section 1021 of the 2012 NDAA—which the government has argued all along—and thereby codifies precisely what the plaintiffs are fighting in court.”) (emphasis in original).

<sup>110</sup> *Hedges v. Obama*, No. 12 Civ. 331 (KBF), 2012 WL 3999839, at \*43 (S.D.N.Y. Sept. 12, 2012); *accord* *Al-Bihani v. Obama*, 590 F.3d 866, 872 (D.C. Cir. 2010) (affirming denial of habeas petition by Guantánamo detainee, based on consideration of MCA “material support” language, and noting that the “provisions of the 2006 and 2009 MCAs are illuminating in this case because the government’s detention authority logically covers a category of persons no narrower than is covered by its military commission authority”).

<sup>111</sup> 2012 WL 3999839, at \*43.

<sup>112</sup> 10 U.S.C. § 950p(a); see 10 U.S.C. § 950p(d) (2009).

<sup>113</sup> See 696 F.3d at 1247–48, 1253.

<sup>114</sup> 125 Stat. at 1562 §§ 1021(a), (d).

with this interpretation,<sup>115</sup> and the judiciary is now weighing in. To the extent NDAA Section 1021(b)(2) does expand executive detention authority, an ex post facto challenge emerges reminiscent of the timeliness analysis in *Hamdan II*.

Although *Hedges* focuses on Fifth Amendment due process, the district court's opinion opens the door to just such an ex post facto challenge. The opinion describes NDAA Section 1021(b)(2) as sufficiently punitive, with the possibility of indefinite military detention as "the equivalent of a criminal penalty," or "perhaps in many circumstances, worse."<sup>116</sup> *Hedges* takes a prospective stance toward that penalty, as plaintiffs alleged a fear of future detention and sought injunctive relief.<sup>117</sup> In rejecting Congress' language as impermissibly vague, the district court found it "reasonable" to interpret the NDAA as drawing "a new, expanded scope for military detention."<sup>118</sup> In fact, in its discussion of plaintiffs' standing, the court disparaged Section 1021 as nothing but "a legislative attempt at an ex post facto 'fix.'"<sup>119</sup> Congress sought to hand the President "broader detention authority than was provided in the AUMF in 2001 and to try to ratify past detentions which may have occurred under an overly-broad interpretation of the AUMF."<sup>120</sup>

The district court's logic is familiar. Just as the MCA expanded the scope of crimes subject to military commission jurisdiction, so too the NDAA expanded the scope of detentions subject to executive authority.<sup>121</sup> Any individuals detained prior to 2012 under a standard of substantial or direct support for terrorism have a new challenge to their detention: that standard was not part of the AUMF, but established over a decade later in the NDAA. Significantly, this challenge can hold even if the appellate court in *Hedges* reverses on grounds that the plaintiffs lack standing.<sup>122</sup> Detainee plaintiffs may come

<sup>115</sup> See Johnson, *supra* note 25 ("[C]ontrary to some reports, neither Section 1021 nor any other detainee-related provision in this year's Defense Authorization Act creates or expands upon the authority for the military to detain a U.S. citizen.").

<sup>116</sup> 2012 WL 3999839, at \*23 n.29; see *id.* at \*\*42, 44; Smith v. Doe, 538 U.S. 84, 92 (2003) (for ex post facto inquiry, court must determine whether legislature intended to impose punishment or to establish civil and nonpunitive statutory scheme).

<sup>117</sup> The district court found standing despite the fact that no plaintiff had been detained, based on plaintiffs' "reasonable fear of detention." 2012 WL 3999839, at \*3; see *id.* at \*\*21, 25–27.

<sup>118</sup> *Id.* at \*21.

<sup>119</sup> *Id.* at \*4; see also *id.* at \*\*16 ("retroactive fix"), 18 ("expansion of detention authority . . . is, for the first time, codified in § 1021").

<sup>120</sup> *Id.* at \*4. The district court felt "required" to wade into interpretive issues concerning the AUMF, given the government's position that the AUMF and NDAA Section 1021(b)(2) are coextensive. *Id.* at \*13.

<sup>121</sup> See *id.* at \*39 ("In other words, the Court finds that § 1021(b)(2) is new.").

<sup>122</sup> The Second Circuit's stay order suggests grounds for reversal based on the plaintiffs' standing, the reach of the NDAA to individuals within the United States, and the scope of the injunction. See Order Granting Stay at 2, *Hedges v. Obama*, Nos. 12-3176 & 12-3644 (2d Cir.

forward. It can also hold even if the court reverses on grounds that NDAA Section 1021(b)(2) satisfies due process. The standard of substantial or direct support may be clear and constitutional going forward, but still inapplicable to previous detentions.<sup>123</sup>

Moreover, the constitutional challenge squarely at issue in *Hedges* benefits from a look back at *Hamdan II*. The Second Circuit Court is poised to decide whether the phrase “substantially supported al-Qaeda, the Taliban, or associated forces . . . [or] directly supported” is sufficiently clear to satisfy due process. Statutory interpretation is delicate business, as the meaning of legislation may be informed by more than the exact words in print. Analogous statutes provide a meaningful context. When construing a statute, the Supreme Court has sought to “achieve a uniform interpretation of similar statutory language” and to respect “congressional policy as expressed in other legislation.”<sup>124</sup> The same guidelines apply to lower federal courts.

To interpret the “substantial or direct support” language of the NDAA, the Second Circuit Court may look to similar statutory provisions. The “material support” language of the MCA is a ready candidate.<sup>125</sup> Both Acts are components of the federal regulatory scheme governing terrorism, with the NDAA addressed to military detention and the MCA addressed to military prosecution.<sup>126</sup> As such, they “should be construed harmoniously.”<sup>127</sup> The MCA has the benefit of clear terminology, incorporating a definition of material support that the Supreme Court recently endorsed.<sup>128</sup> After *Hamdan II*, it also

---

Oct. 2, 2012) (No. 78).

<sup>123</sup> Cf. *Hamdan II*, 696 F.3d at 1241 n.1. During oral argument on the *Hedges* appeal, U.S. District Judge Lewis Kaplan, sitting on the Second Circuit panel by designation from the Southern District of New York, hinted that he may vote in favor of the government’s position. See Klasfeld, *supra* note 106. Plaintiffs-Appellees’ attorney Carl Mayer invoked the district court’s view that “there would be no reason for a law to codify existing law.” *Id.* Judge Kaplan responded by invoking NDAA Section 1021(e), which provides that “[n]othing in this section shall be construed to affect existing law,” and stating, “It seems to me you might have an insurmountable problem.” *Id.*; 125 Stat. at 1562 § 1021(e).

<sup>124</sup> *Rodriguez de Quijas v. Shearson/American Exp., Inc.*, 490 U.S. 477, 484 (1989) (explaining Court’s willingness to overturn its own decisions construing statutes, despite force of stare decisis).

<sup>125</sup> See 10 U.S.C. § 950v(b)(25); 10 U.S.C. § 950(t)(25) (2009).

<sup>126</sup> Also within this regulatory scheme are the AUMF, providing for the use of force, and 18 U.S.C. §§ 2339A–2339B, providing for federal prosecution of material support for terrorism.

<sup>127</sup> *Rodriguez de Quijas*, 490 U.S. at 484–85 (construing terms in Securities Act of 1933 and Securities Exchange Act of 1934).

<sup>128</sup> See *Holder v. Humanitarian Law Project*, 130 S. Ct. 2705 (2010). There, the Court rejected a vagueness challenge to the material-support statute, 18 U.S.C. § 2339B, brought by activists supporting humanitarian and political causes in Turkey and Sri Lanka. See 130 S. Ct. at 2720–22. Both Section 2339B and the MCA rely on the same definition of “material support or resources.” Compare 18 U.S.C. § 2339B(g)(4) with 10 U.S.C. § 950v(25)(B) and 10 U.S.C.

carries the D.C. Circuit Court's stamp of approval for timely charges.

#### V. CONCLUSION

Therefore, far from undermining the legitimacy of Guantánamo military commissions, *Hamdan II* fosters a richer understanding of the proceedings. Perhaps most significant in this sensational opinion is the lack of anything sensationalist. By offering an ordinary appellate analysis in the extraordinary context of Guantánamo, the D.C. Circuit Court has placed a military commission judgment squarely in line with district court judgments. *Hamdan II* stands as a reminder that principles of fairness apply in military and civilian trials alike.



## ARTICLE

# Non-State Armed Groups and Technology: The Humanitarian Tragedy at Our Doorstep?

Colonel Dave Wallace & Major Shane Reeves\*

### Abstract

*Technological advances are altering the contemporary asymmetric conflicts between non-state armed groups and state actors. This article discusses the humanitarian consequences of these changing conflicts by first illustrating the dangers posed by non-state armed groups gaining access to advanced technologies. A subsequent examination of the increasing ability of non-state armed groups to use new technologies, such as cyber operations, to mitigate state actor advantages and the resultant risks to civilian populations follows. The article concludes that the humanitarian challenges presented by this growing intimacy between non-state armed groups and technology, whether through a potentially devastating attack or by the dramatic erosion to the principle of distinction, are immense and cannot be ignored.*

*In most wars, the same laws and principles hold true for each contending side. What varies is the way each opponent uses them, according to his ability, his particular situation, and his relative strength. Conventional war belongs to this general case. Revolutionary war, on the other hand, represents an exceptional case not only because, as we suspect, it has its special rules, different from those of the conventional war, but also because most of the rules applicable to one side do not work for the other. In a fight between a fly and a lion, the fly cannot deliver a knockout blow and the lion cannot fly. It is the same war for both camps in terms of space and time, yet there are two distinct 'warfare's—the revolutionary's and, shall we say, the counterrevolutionary's.<sup>1</sup>*

---

Colonel Dave Wallace is a Professor and the Deputy Head, Department of Law at the United States Military Academy, West Point, New York. Major Shane Reeves is an Assistant Professor at the United States Military Academy, West Point. The views expressed here are their personal views and do not necessarily reflect those of the Department of Defense, the United States Army, the United States Military Academy, or any other department or agency of the United States Government. The analysis presented here stems from their academic research of publicly available sources, not from protected operational information.

<sup>1</sup> DAVID GALULA, COUNTERINSURGENCY WARFARE: THEORY AND PRACTICE xii-xiii (Praeger Sec. Int'l 2006) (1964).

## Table of Contents

---

I. INTRODUCTION.....	27
II. HOW ARMED GROUPS USE NEW TECHNOLOGY AND WHY.....	29
A. <i>Drone Warfare</i> .....	30
B. <i>Weapons of Mass Destruction</i> .....	32
C. <i>Missile Technology</i> .....	33
D. <i>Improvised Explosive Devices (IEDs)</i> .....	34
E. <i>Information Technology</i> .....	36
III. COUNTERING NEW TECHNOLOGY WITH TECHNOLOGY.....	38
IV. CONCLUSION.....	45

### I. INTRODUCTION

The paradoxes and dilemmas of armed conflict are constant<sup>1</sup> with these contradictions and puzzles readily apparent in asymmetrical warfare. Asymmetric warfare is defined as “leveraging inferior tactical or operational strength against the vulnerabilities of a superior opponent to achieve a disproportionate effect with the aim of undermining the opponent’s will in order to achieve the asymmetric actor’s strategic objectives.”<sup>2</sup> The phenomenon, and challenge, of asymmetrical warfare is certainly not new: the earliest recorded example is contained in the Old Testament of the Bible as the fight between David and Goliath.<sup>3</sup>

Non-state armed groups practice asymmetric warfare, to a great extent, as a result of the technological superiority historically enjoyed by state actors.<sup>4</sup> However, state actors increasingly do not have a monopoly on advanced technologies as “globalization has transformed the process of technological innovation while lowering entry barriers for a wider range of actors to acquire

---

<sup>1</sup> MICHAEL L. GROSS, *MORAL DILEMMAS OF MODERN WARFARE – TORTURE, ASSASSINATION, AND BLACKMAIL IN THE AGE OF ASYMMETRIC CONFLICT* 21 (Cambridge Press, 2010).

<sup>2</sup> Kenneth F. McKenzie Jr., *The Rise of Asymmetric Threats: Priorities for Defense Planning*, in NAT’L DEF. UNIV., QDR 2001 STRATEGY-DRIVEN CHOICES FOR AMERICA’S SECURITY 75, 76 (Michele A. Flournoy ed., 2001).

<sup>3</sup> K.C. Dixit, *The Challenges of Asymmetric Warfare*, Institute for Defense Studies and Analysis, IDSA Comment, (Mar. 9, 2010), [http://www.idsa.in/idsacomments/TheChallengesofAsymmetricWarfare\\_kcdixit\\_090310](http://www.idsa.in/idsacomments/TheChallengesofAsymmetricWarfare_kcdixit_090310).

<sup>4</sup> See, e.g., U.S. DEP’T OF ARMY, FIELD MANUAL 3–24/U.S. MARINE CORPS WARFIGHTING PUBLICATION 3–33.5, COUNTERINSURGENCY ix (2006) [hereinafter FM 3–24] (“The United States possesses overwhelming conventional military superiority. This capability has pushed its enemies to fight U.S. forces unconventionally, mixing modern technology with ancient techniques of insurgency and terrorism. Most enemies either do not try to defeat the United States with conventional operations or do not limit themselves to purely military means.”).

advanced technologies.”<sup>5</sup> As a result “non-state actors continue to gain influence and capabilities that, during the past century, remained largely the purview of states.”<sup>6</sup> This unprecedented access to advanced technologies most likely is not enough to alter non-state armed groups’ adherence to asymmetric warfare, but it does provide new ways for these groups to leverage their limited strengths “against the vulnerabilities of [their] superior opponent” in order to eventually achieve their strategic objectives.<sup>7</sup>

Regardless of potential access to new technologies, non-state armed groups are cognizant that state actors currently retain a technological advantage. This advantage is not insignificant as state actors are able to use technology to tip the scales heavily in their favor in contemporary military operations.<sup>8</sup> Non-state armed groups are therefore constantly searching for effective counter measures to minimize the technological superiority of the state actor. Perhaps nothing is more effective as a mitigation measure than a non-state armed group’s willingness to ignore the Law of War’s<sup>9</sup> sacrosanct protections for the civilian population and civilian objects<sup>10</sup> in order to reduce their operational

---

<sup>5</sup> U.S. DEP’T OF DEF., QUADRENNIAL DEFENSE REVIEW REPORT EXECUTIVE SUMMARY iv, (2010) *available at* [http://www.defense.gov/qdr/images/QDR\\_as\\_of\\_12Feb10\\_1000.pdf](http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf) [hereinafter QDR].

<sup>6</sup> *Id.*

<sup>7</sup> McKenzie Jr., *supra* note 3, at 76. In asymmetric warfare the ‘weaker’ actor will maximize the use of their limited resources in order to negatively impact the psychological strength of the ‘stronger’ actor. *Id.* As non-state armed groups acquire advanced technology, they will most likely attempt to “compensate for material or other deficiencies” by using previously unattainable weaponry to affect the morale and will of the state actor. *Id.* at 77.

<sup>8</sup> *See, e.g.,* Gregory Viscusi & David Lerman, *French Air Power Begins, Ends NATO Campaign Over Libya With Sarkosky’s Help*, BLOOMBERG (Oct. 20, 2011),

<http://www.bloomberg.com/news/2011-10-20/french-air-power-begins-ends-nato-air-campaign-over-libya.html> (describing the critical importance of NATO air superiority in the toppling of the Qaddafi regime); Mark Mazzetti, Eric Schmitt, & Robert F. Worth, *Two Year Manhunt Led to Killing of Awlaki in Yemen*, N.Y. TIMES, Sept. 30, 2011, <http://www.nytimes.com/2011/10/01/world/middle-east/anwar-al-awlaki-is-killed-in-yemen.html?pagewanted=all> (discussing the lethal capabilities of the U.S. drone program).

<sup>9</sup> *See* U.S. DEP’T OF DEF., DIRECTIVE 2311.01E: DOD LAW OF WAR PROGRAM, ¶ 3.1 (2006), *available at* <http://www.dtic.mil/whs/directives/corres/pdf/231101e.pdf> (defining the law of war as the part of international law that regulates the “conduct of armed hostilities” and is often called “the law of armed conflict”). The law of war, the law of armed conflict, and international humanitarian law are interchangeable. For the remainder of this article, we will use the term “law of war” as this traditional term clearly notates the *lex specialis* that governs during a time of armed conflict.

<sup>10</sup> *See* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict (Protocol I) art. 48, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I] (“In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives . . .”).



risks.<sup>11</sup>

Exacerbating this humanitarian problem is the growing ability of non-state armed groups to discreetly and effectively conduct on-going operations while living amongst unsuspecting civilian populations. Advanced technology, and, in particular the rapid evolution of cyberspace, allows these groups to disperse widely across the globe without degrading their capabilities or agenda.<sup>12</sup> The threat to longstanding international norms and civilian populations by these tactics is obvious. Similarly, as non-state armed groups gain access to significantly advanced and lethal technology, they will not hesitate to target civilian populations if they believe this will exploit the weakness of their superior state actor foes.<sup>13</sup> The humanitarian consequences of non-state armed groups trying to “level the playing field” with state actors by either pursuing, or mitigating, advanced technology are therefore potentially devastating.

To support these propositions this article will first illustrate the humanitarian concerns posed by non-state armed groups gaining access to advanced technologies. A discussion of the erosion of civilian protections by non-state armed groups in an asymmetric war and the subsequent humanitarian risks will follow. Finally, the article will briefly summarize the uncertain humanitarian challenges facing the international community by the arrival of ever increasing advanced technology.

## II. HOW ARMED GROUPS USE NEW TECHNOLOGY AND WHY

Asymmetric warfare encompasses a wide scope of theory, experience, conjecture, and definition. The underlying premise is that asymmetric warfare deals with unknowns, with surprise in terms of ends, ways, and means. As Professor Michael Schmitt insightfully notes, the asymmetry of warfare has

---

<sup>11</sup> See, e.g., Human Rights Council, *Human Rights in Palestine and Other Occupied Arab Territories: Report of the United Nations Fact Finding Mission on the Gaza Conflict*, ¶¶ 439–98. U.N. Doc. A/HRC/12/48 (Sept. 15, 2009) [hereinafter Goldstone Report], available at [http://www2.ohchr.org/english/bodies/hrcouncil/specialsession/9/docs/UNFFMGC\\_Report.pdf](http://www2.ohchr.org/english/bodies/hrcouncil/specialsession/9/docs/UNFFMGC_Report.pdf) (detailing the various ways in which Palestinian Armed Groups violated the law of war in order to mitigate the conventional superiority of the Israeli Armed Forces).

<sup>12</sup> See Kelly Gables, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 43 VAND. J. TRANSNAT’L L. 57, 57 (2010) (“The Internet not only makes it easier for terrorists to communicate, organize terrorist cells, share information, plan attacks, and recruit others but also is increasingly being used to commit cyberterrorist acts. It is clear that the international community may only ignore cyberterrorism at its peril.”).

<sup>13</sup> See, e.g., Al-Qaeda’s Fatwa (Feb. 23, 1998), available at [http://www.pbs.org/newshour/updates/military/jan-june98/fatwa\\_1998.html](http://www.pbs.org/newshour/updates/military/jan-june98/fatwa_1998.html) (“The ruling to kill the Americans and their allies—civilians and military—is an individual duty for every Muslim who can do it in any country in which it is possible to do it . . .”).

many dimensions. That is, it operates across the spectrum of conflict from the tactical through the strategic levels of war. Asymmetry is also manifested in various forms: technological, doctrinal, normative, participatory and legal/moral.

Armed groups attempt to “balance the playing field” against states and their armed forces by using (or attempting to use) various means of warfare, including: unmanned aerial vehicles, weapons of mass destruction, surface-to-air missiles, information technology, and improvised explosive devices.

#### A. *Drone Warfare*

Drones are unmanned aerial vehicles that are remotely controlled by “pilots” who may be thousands of miles away from where the drone is flying.<sup>14</sup> In the air domain, drones are used to engage in reconnaissance and surveillance missions, to facilitate communications and locate and acquire targets.<sup>15</sup> By any measure, drones have proven to be extraordinarily successful in finding and killing targeted enemies<sup>16</sup> becoming a prevalent aspect of airpower.<sup>17</sup> Since 2001, drones have increasingly been the counter-terrorism weapons of choice. In that year, the U.S. Predator drone fleet numbered about ten; their mission set was generally limited to reconnaissance missions.<sup>18</sup> Since 2005, there has been a 1,200 percent increase in drone combat air patrols by the United States<sup>19</sup> with American intelligence officials call drones their most effective weapon against al-Qaeda and the Taliban.<sup>20</sup> Hardly a month passes without a report that another enemy leader has been killed by a drone-launched Hellfire missile.<sup>21</sup> With names like Predator, Global Hawk, Shadow, Raven and Wasp, these drones are an indispensable part of the U.S. efforts in Afghanistan and Iraq.<sup>22</sup>

---

<sup>14</sup> Mary Ellen O’Connell, *The Resort to Drones Under International Law*, 39 DENV. J. INT’L L. & POL’Y 585, 585(2011).

<sup>15</sup> WILLIAM H. BOOTHBY, *WEAPONS AND THE LAW OF ARMED CONFLICT* 229 (2009).

<sup>16</sup> Ryan J. Vogel, *Drone Warfare and the Law of Armed Conflict*, 39 DENV. J. INT’L L. & POL’Y 101, 102 (2011).

<sup>17</sup> ROD THORNTON, *ASYMMETRIC WARFARE*, 94 (2010).

<sup>18</sup> *Id.* at 104.

<sup>19</sup> *Flight of the Drones*, ECONOMIST, October 8, 2011, available at <http://www.economist.com/node/21531433>.

<sup>20</sup> *Predator Drones and Unmanned Aerial Vehicles (UAVs)*, N.Y. TIMES, [http://topics.nytimes.com/top/reference/timestopics/subjects/u/unmanned\\_aerial\\_vehicles/index.html](http://topics.nytimes.com/top/reference/timestopics/subjects/u/unmanned_aerial_vehicles/index.html) (last updated July 30, 2012).

<sup>21</sup> See *Flight of the Drones*, *supra* note 22.

<sup>22</sup> See generally P.W. Singer, *Military Robots and the Law of War*, NEW ATLANTIS, Winter 2009, available at <http://www.thenewatlantis.com/publications/military-robots-and-the-laws-of-war>.

Drone technology is spreading rapidly with estimates of up to 50 countries developing or purchasing these systems.<sup>23</sup> Countries including Israel and the UK have used drones for combat operations while others only use them for surveillance purposes. China, for example, debuted a small drone equipped with a high-definition camera at a robotics trade show.<sup>24</sup> Of great concern are the growing commonality of drones and the increasing ability of non-state armed groups to acquire this technology.

Hezbollah reportedly deployed an Iranian-designed drone<sup>25</sup> and allegedly flew at least three Mirsad (Arabic for 'ambush') drones into Israel with each carrying a payload of approximately twenty-two pounds of explosives, packed with ball bearings.<sup>26</sup> A Hezbollah leader, bragging at a rally about targeting Israel, stated "[y]ou can load the Mirsad plane with a quantity of explosive ranging from 40 to 50 kilos and send it to its target, . . . do you want a power plant, water plant, military base? Anything!"<sup>27</sup> P.W. Singer notes that the use of drones is not limited to large-scale non-state armed groups, such as Hezbollah, and that more obscure groups are increasingly able to use or develop such technology.<sup>28</sup>

Contractors, such as the group previously known as Blackwater, added a section to their business seeking to rent out drones.<sup>29</sup> Additionally, drones have a number of commercial purposes increasing their proliferation around the world. Accordingly, non-state groups have greater access to such technology and their ability to use them is only limited by their imagination. For example, such groups could, in a cost effective manner, use drone technology to precisely attack otherwise hard to reach targets. Such attacks could even be aimed at critical infrastructure or the civilian population using weapons of mass destruction. Put differently, such armed groups could leverage drone technology to do far more damage, real and psychological, than

---

<sup>23</sup> See David Cortright, *The Scary Prospect of Global Drone Warfare*, CNN OPINION, <http://www.cnn.com/2011/10/19/opinion/cortright-drones/index.html> (last updated Oct. 14, 2011).

<sup>24</sup> Brianna Lee, *Things You Need to Know About Drones*, PBS, available at <http://www.pbs.org/wnet/need-to-know/five-things/drones/12659>.

<sup>25</sup> David Cortright, *The Scary Prospect of Global Drone Warfare*, CNN OPINION, <http://www.cnn.com/2011/10/19/opinion/cortright-drones/index.html> (last updated Oct. 14, 2011).

<sup>26</sup> P.W. SINGER, *WIRED FOR WAR*, 264 (2009).

<sup>27</sup> *NBC Nightly News: Hezbollah drone threatens Israel* (NBC television broadcast Apr. 12, 2005), available at [http://www.msnbc.msn.com/id/7477528/ns/nightly\\_news/t/hezbollah-drone-threatens-israel/](http://www.msnbc.msn.com/id/7477528/ns/nightly_news/t/hezbollah-drone-threatens-israel/).

<sup>28</sup> See SINGER, *supra* note 29, at 265.

<sup>29</sup> *Id.*

they could ever do with a suicide attack or a car filled with explosives.<sup>30</sup>

### *B. Weapons of Mass Destruction*

Nuclear, chemical, and biological weapons are inherently terrorizing<sup>31</sup> and are the weapons state actors fear the most in the hands of non-state actors.<sup>32</sup> No other weapons can “level the playing field” between non-state armed groups and state actors as these weapons of mass destruction have the potential to kill millions of people quickly with relative ease.<sup>33</sup> In one of the many paradoxes of asymmetrical warfare, non-state actors can, and will, likely use such weapons if obtained, while their state adversaries, who already possess these weapons, cannot, and will not, use them.<sup>34</sup>

There have been reports that non-state armed groups continue to attempt to acquire such weapons. For example, “al-Qaeda’s top leadership has demonstrated a sustained commitment to buy, steal or construct weapons of mass destruction.”<sup>35</sup> In late 2001, Ayman Zawahiri stated, “[i]f you have \$30 million, go to the black market in the central Asia, contact any disgruntled Soviet scientist and a lot of dozens of smart briefcase bombs are available.”<sup>36</sup> Al-Qaeda announced its goal to “kill four million Americans” a few months later.<sup>37</sup> Osama bin Laden reportedly paid \$1.5 million to a Sudanese military officer and acquired a uranium canister in 1993, which he hoped could be used as a mass destruction weapon.<sup>38</sup> In 1998, bin Laden declared that acquiring and using weapons of mass destruction was his Islamic duty and dispatched his senior operatives to attempt to purchase or develop nuclear and biochemical weapons of mass destruction.<sup>39</sup>

---

<sup>30</sup> Eugene Miasnikov, *Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects*, in CENTER FOR ARMS CONTROL, ENERGY AND ENVIRONMENTAL STUDIES MOSCOW INSTITUTE OF PHYSICS AND TECHNOLOGY 4 (2005), <http://www.armscontrol.ru/uav/uav-report.pdf>.

<sup>31</sup> Jessica Stern, *Getting and Using the Weapons*, in TERRORISM AND COUNTERTERRORISM 182 (Russell B. Howard & Reid Sawyer eds. 2004).

<sup>32</sup> See THORNTON, *supra* note 20, at 33 (stating that non-state actors are capable of inflicting massive casualties and generating significant panic with weapons of mass destruction).

<sup>33</sup> DAN CALDWELL & ROBERT E. WILLIAMS, JR., SEEKING SECURITY IN AN INSECURE WORLD 49 (2006).

<sup>34</sup> THORNTON, *supra* note 20, at 33.

<sup>35</sup> Graham Allison, *Foreword to Rolf Mowatt-Larssen, Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality*, Belfer Ctr. for Sci. and Int'l Affairs, John F. Kennedy Sch. of Gov't (Jan. 2010), <http://belfercenter.ksg.harvard.edu/files/al-qaeda-wmd-threat.pdf>.

<sup>36</sup> *Id.*

<sup>37</sup> *Id.*

<sup>38</sup> See ROHAN GUNARATNA & PETER CHALK, JANE'S COUNTER TERRORISM 41 (2002) (noting that al-Qaeda went so far as to test the canister with a Geiger counter to ensure it was radioactive).

<sup>39</sup> Rolf Mowatt-Larssen, *Al Qaeda's Pursuit of Weapons of Mass Destruction*, FOREIGN POLICY (Jan. 25, 2010) available at [http://www.foreignpolicy.com/articles/2010/01/25/al\\_qaedas\\_pursuit\\_of\\_weapons\\_of\\_mass\\_](http://www.foreignpolicy.com/articles/2010/01/25/al_qaedas_pursuit_of_weapons_of_mass_)

Non-state armed groups besides al-Qaeda, also use, or covet, weapons of mass destruction. For example, LTTE rebels (the Tamil Tigers), employed chlorine gas against a detachment of the Sri Lankan armed forces in Kiran, Eastern Sri Lanka obtaining the gas from a nearby paper mill.<sup>40</sup> Recalling the attack, an officer said, “[e]verything was dark when it exploded [reflecting his belief that the chemical weapon was delivered by mortar-fired projectiles], but there was a huge smoke, it was like when you set a fire. The ground was blackened where the projectiles hit.”<sup>41</sup> On November 23, 1995, Chechen separatists placed a bomb containing 70 pounds of a mixture of cesium-137 and dynamite in Moscow’s Ismailovsky Park.<sup>42</sup> Ultimately, the Chechen rebels opted not to explode the dirty bomb but instead informed the media of its location.<sup>43</sup>

The perceived threat of WMD use by non-state groups has been increased dramatically since the end of the Cold War.<sup>44</sup> Author Andrew O’Neill offered three reasons for this phenomenon. First, with the collapse of the Soviet Union in 1991, there has been significant concern about the physical security of the weapons of mass destruction in the territories of the former Soviet Union.<sup>45</sup> The second reason is the emergence of a new breed of non-state armed groups who are more likely to use lethal and indiscriminate forms of violence. Finally, the transnational nature of these groups makes no location, as illustrated by the attacks of September 11<sup>th</sup>, beyond their reach.<sup>46</sup>

### C. Missile Technology

In 1986, the United States armed the Afghan Mujahideen with Stinger anti-aircraft missiles to help them combat the Soviet Union.<sup>47</sup> At the time, the Stinger was considered a highly effective hand-held anti-aircraft missile

---

destruction?hidecomments=yes.

<sup>40</sup> See GUNARATNA & CHALK, *supra* note 41, at 42.

<sup>41</sup> Bruce Hoffman, *The first non-state use of a chemical weapon in warfare: the Tamil Tigers' assault on East Kiran*, 20 SMALL WARS & INSURGENCIES 463, 470 (2009), available at <http://www.tandfonline.com/doi/full/10.1080/09592310903026969#tabModule>.

<sup>42</sup> Graham Allison, *Nuclear Terrorism: How Serious a Threat to Russia?* RUSSIA IN GLOBAL AFFAIRS, Sept./Oct., (2004), available at [http://belfercenter.ksg.harvard.edu/publication/660/nuclear\\_terrorism.html](http://belfercenter.ksg.harvard.edu/publication/660/nuclear_terrorism.html).

<sup>43</sup> *Id.*

<sup>44</sup> Andrew O’Neil, *Terrorist Use of Weapons of Mass Destruction: How Serious Is the Threat?*, 57 AUSTL. J. OF INT’L AFF. 99, 100 (2003) (arguing that even though WMD terrorism remains a real prospect, the ease with which such attacks can be carried out has been exaggerated).

<sup>45</sup> *Id.*

<sup>46</sup> *Id.*

<sup>47</sup> Alan J. Kuperman, *The Stinger Missile and the U.S. Intervention into Afghanistan*, 114 POL. SCI. Q. 219, 219 (1999).

capable of locking onto the heat signature of a helicopter or airplane engine. In his book, *Holy War, Inc.*, author Peter L. Bergen noted once the Stinger missiles were deployed into the hands of the Mujahideen, the Soviets lost the air superiority they had previously enjoyed. Ahmad Shah Massoud, an Afghan military leader who played a leading role in driving the Soviet army out of Afghanistan once quipped, "[t]here are only two things the Afghan must have: the Koran and Singers."<sup>48</sup>

Shoulder-fired surface-to-air missiles in the hands of non-state actors pose a significant threat to passenger air travel, the commercial aviation industry, and military aircraft around the world. Since the 1970s, there have been over 40 civilian aircraft hit by such missiles.<sup>49</sup> It is believed that two dozen armed groups have gained access to surface-to-air missiles with the most popular remaining the shoulder-fired heating missiles.<sup>50</sup> Of great concern today is the possibility of a state collapse allowing their conventional arsenal, including such missiles, to slip into the hands of non-state armed groups.<sup>51</sup>

#### *D. Improvised Explosive Devices (IEDs)*

Often used by non-state actors who wage non-traditional warfare, so-called improvised explosive devices or IEDs can be made from almost any material and are designed to kill or maim.<sup>52</sup> Improvised explosive devices are the most lethal weapons of non-state groups participating in the conflicts of Afghanistan and Iraq. In Iraq, IEDs are responsible for two-thirds of coalition deaths while in Afghanistan such attacks have roughly tripled in the past two years.<sup>53</sup> Improvised explosive devices are global threats. From January to November 2011, outside of Iraq and Afghanistan, there have been 6,832 improvised explosive events in 111 countries resulting in 12,286 casualties. Such attacks were carried out by 40 regional and transnational threat networks of non-state

---

<sup>48</sup> PETER L. BERGEN, *HOLY WAR, INC.: INSIDE THE SECRET WORLD OF OSAMA BIN LADEN* (2001).

<sup>49</sup> See Fact Sheet, U.S. Dep't of State, *MANPADS: Combating the Threat to Global Aviation from Man-Portable Air Defense Systems* (July 31, 2008), <http://merln.ndu.edu/archivepdf/terrorism/state/107632.pdf>.

<sup>50</sup> See GUNARATNA & CHALK, *supra* note 41, at 642.

<sup>51</sup> See, e.g., Addison Wiggin, *Where Will Libya's Shoulder-Fired Missiles Land?*, FORBES (Sept. 29, 2011), <http://www.forbes.com/sites/greatspeculations/2011/09/29/where-will-libyas-shoulder-fired-missiles-land/> (discussing the great concern that the 20,000 missiles possessed by Libya at the time of the government's collapse would find their way into the hands of terrorists).

<sup>52</sup> See *Improvised Explosive Devices*, N.Y. TIMES TOPICS, [http://topics.nytimes.com/topics/reference/timestopics/subjects/i/improvised\\_explosive\\_devices/index.html?offset=0&s=newest](http://topics.nytimes.com/topics/reference/timestopics/subjects/i/improvised_explosive_devices/index.html?offset=0&s=newest) (last visited Feb. 20, 2012).

<sup>53</sup> See *Bombs Away*, ECONOMIST, (Mar. 4, 2010), available at <http://www.economist.com/node/15582147>.

actors.<sup>54</sup>

Because of the on going and increasing threat by IEDs in Iraq and Afghanistan, the United States established the Joint IED Defeat Organization, known as JIEDDO in February 2006.<sup>55</sup> In JIEDDO's Strategic Plan (2012-2016), Lieutenant General Michael Barbero stated:

The IED is the weapon of choice for the overlapping consortium of networks operating along the entire threat continuum — criminal, insurgent, and terrorist alike. Threat networks use IEDs because they are cheap, readily available, easy to construct, lethal, and effective. The IED is a weapon used strategically to cause casualties, create the perception of insecurity, and influence national will. This threat is complex and transnational in nature, representing layers of interdependent, inter-connected global threat networks, and support systems.<sup>56</sup>

A basic IED has four components: an explosives charge, an initiator, a power source and an activation switch.<sup>57</sup> Most IEDs used by non-state actors are decidedly low-tech, jury-rigged affairs consisting of a few command wires, some fertilizer chemicals and wooden pressure plates. Others consist of leftover mines or plastic explosives that are detonated remotely by a cellphone.<sup>58</sup> However, not all IEDs are simple; non-state groups are becoming increasingly sophisticated in their design and production, particularly in terms of explosively formed projectiles and advanced triggers, which have caused disproportionate levels of casualties relative to the numbers of such devices employed.<sup>59</sup> An example from the conflict in Iraq illustrates this point. With the help of the Iranians, insurgents in Iraq deployed deadly devices known as explosively formed projectile (EFPs).<sup>60</sup> This type of IED is typically made from a pipe containing explosives and capped by a copper disk. When detonated, the copper disk is transformed into a molten jet of metal capable of penetrating

---

<sup>54</sup> Spencer Ackerman, *Pentagon: Future of Homemade Bombs Is High-Tech*, WIRED MAGAZINE (Feb. 14, 2012, 2:30 PM), <http://www.wired.com/dangerroom/2012/02/jieddo-high-tech-bombs/> (citing *Counter Improvised Explosive Device Strategic Plan*, JOINT IMPROVISED EXPLOSIVE DEVICE DEFEAT ORG. 2012-2016, 1–2 (Jan. 1, 2012), [hereinafter JIEDDO], available at <http://www.globalsecurity.org/military/library/policy/dod/jieddo-cied-plan-120116.pdf> (last visited Sept. 30, 2012)).

<sup>55</sup> See generally U.S. DEP'T OF DEF., DIRECTIVE 2000.19E, JOINT IMPROVISED EXPLOSIVE DEVICE DEFEAT ORGANIZATION (JIEDDO), available at <http://www.dtic.mil/whs/directives/corres/pdf/200019p.pdf>.

<sup>56</sup> See JIEDDO, *supra* note 57, at iii.

<sup>57</sup> See GUNARATNA & CHALK, *supra* note 41, at 29.

<sup>58</sup> See JIEDDO, *supra* note 57, at iii.

<sup>59</sup> *Id.*

<sup>60</sup> Tom Vanden Brook, *U.S. Blames Iran for New Bombs in Iraq*, USA TODAY (Jan. 30, 2007, 9:45 PM), [http://www.usatoday.com/news/world/iraq/2007-01-30-ied-iran\\_x.htm](http://www.usatoday.com/news/world/iraq/2007-01-30-ied-iran_x.htm).

armor thus operating the same as a U.S. anti-tank missile.<sup>61</sup>

The leading authorities on improvised explosive devices, JIEDDO, paint an alarming picture of the advances in IED technology. More specifically, it reports:

In the future, devices will adopt ever more sophisticated technology, limited only by the terrorists' imaginations. . . .Future bomb makers will seek to incorporate such enhancements as peroxide- and hydrogen-based explosives; nanotechnology and flexible electronics; new forms of power, e.g., microbial fuel cells, non-metallic and solar; advanced communications (Bluetooth, 4G, Wi-Fi, broadband); optical initiators (using laser or telemetry more than infrared); and highly energetic and molecular materials. Indicators have shown that terrorist networks which innovate with these new technologies are also developing enhanced IED concealment techniques and may even combine IED use with concurrent cyber attacks. Bomb makers will take advantage of available technology and innovate in response to countermeasures — weapons will be more lethal and harder to detect and defeat.<sup>62</sup>

#### *E. Information Technology*

Information technology has revolutionized warfare and is central to state actor military dominance.<sup>63</sup> Such technology as the Global Positioning System, communications capabilities, sensors, advanced radar/sonar, cyber warfare capabilities, guided munitions, and much more have seemingly widened the capabilities gap with non-state armed groups. The paradox of a conflict between a state actor and anon-state armed groups is that such modern technology is both the great separator and the great equalizer.<sup>64</sup> Non-state groups, like al-Qaeda, Hezbollah, Iraqi insurgents and others, thrive in the information age because they are able to exploit—or threaten to—exploit many of the same information technologies that make state militaries so powerful. Such non-state armed groups have been stunningly innovative in their exploitation of technology.<sup>65</sup> Additionally, the more powerful the economy or military organization, the more likely they will rely on information technology,

---

<sup>61</sup> *Id.*

<sup>62</sup> JIEDDO, *supra* note 57, at 4.

<sup>63</sup> See Max Boot, *The Paradox of Military Technology*, NEW ATLANTIS, Fall 2006, available at <http://www.thenewatlantis.com/publications/the-paradox-of-military-technology> (noting that the United States has the most advanced weapons systems and sophisticated information technology in world; however, such technology is not a perfect shield against other kinds of destructive power).

<sup>64</sup> *Id.* (According to Boot, technological supremacy separates the United States from the rest of the world, and yet modern technology leaves America vulnerable to vicious groups and gangs armed with AK47s, car bombs, or portable WMDs).

<sup>65</sup> See SINGER, *supra* note 29, at 264.



which results in a greater vulnerability.<sup>66</sup>

In 2006, in the midst of an armed conflict with Israel in southern Lebanon, Hezbollah fighters were able to hack into the Israeli Army's computer and radio systems.<sup>67</sup> According to some reports, with the intelligence gained through the intercepts, Hezbollah was able to thwart Israeli tank assaults.<sup>68</sup> It is believed that Hezbollah used Iranian-supplied technology to accomplish this feat.<sup>69</sup> Commenting on the incident, author P.W. Singer stated that, "[n]otably, the group's Internet attacks on Israel originally appeared to come from a small south Texas cable company, a suburban Virginia cable provider and web-hosting servers in Delhi, Montreal, Brooklyn, and New Jersey. But these all had actually been 'hijacked' by Hezbollah hackers."<sup>70</sup>

Non-state armed groups fighting against coalition forces in Iraq and Afghanistan have also used information technology with great skill. Such groups post videos of their exploits on the Internet while also communicating through mobile phones, e-mails, and websites.<sup>71</sup> The Taliban is even using Twitter to wage war against the United States.<sup>72</sup> In Iraq, tech savvy insurgents use the Internet to recruit suicide bombers, spread propaganda, and even publish monthly online magazines.<sup>73</sup>

Cyberspace is now a war zone where many of the decisive battles of the twenty-first century will be played out.<sup>74</sup> The United States Department of Defense's Quadrennial Defense Review Report defines cyberspace as "a global domain within the information environment that encompasses the interdependent networks of information technology infrastructures, including

---

<sup>66</sup> See THORNTON, *supra* note 20, at 55 (discussing the challenges and threats of asymmetric warfare in the 21st century).

<sup>67</sup> See SINGER, *supra* note 29, at 264.

<sup>68</sup> E.g. Mohamad Bazzi, *Hezbollah Cracked the Code*, NEWSDAY (Sept. 17, 2006, 8:00 PM), <http://www.newsday.com/news/hezbollah-cracked-the-code-1.681121>.

<sup>69</sup> See John Leyden, *Hezbollah Cracks Israeli Radio Code*, THE REGISTER (Sept. 20, 2006, 13:06 GMT), [http://www.theregister.co.uk/2006/09/20/hezbollah\\_cracks\\_israeli\\_radio/](http://www.theregister.co.uk/2006/09/20/hezbollah_cracks_israeli_radio/).

<sup>70</sup> SINGER, *supra* note 29, at 264.

<sup>71</sup> See Michelle Nichols, *Tech-savvy Taliban Fights War in Cyberspace*, REUTERS (July 20, 2011, 4:13 AM), <http://www.reuters.com/article/2011/07/20/us-afghanistan-taliban-technology-idUSTRE76J1HL20110720>.

<sup>72</sup> Ernesto Londoño, *U.S. Military, Taliban Use Twitter to Wage War*, WASHINGTON POST, (Dec. 18, 2011), [http://www.washingtonpost.com/world/asia\\_pacific/us-military-taliban-use-twitter-to-wage-war/2011/12/16/gIQAknJ320\\_story.html](http://www.washingtonpost.com/world/asia_pacific/us-military-taliban-use-twitter-to-wage-war/2011/12/16/gIQAknJ320_story.html) (stating that the International Security Assistance Force engages in a "near-daily battle" with the Taliban on Twitter).

<sup>73</sup> See Jonathan Curiel, *Terror.Com / Iraq's Tech-savvy Insurgents Are Finding Supporters and Luring Suicide-bomber Recruits over the Internet*, SFGATE (July 10, 2005, 4:00 AM), <http://www.sfgate.com/news/article/TERROR-COM-Iraq-s-savy-insurgents-are-2623261.php>.

<sup>74</sup> See RICHARD A. CLARKE, *CYBER WAR*, 69 (2010).

the Internet and telecommunication networks.”<sup>75</sup> Cofer Black, former head of the Central Intelligence Agency's Counter Terrorism Center, recently noted that it is likely that we will see more cyber attacks from al-Qaeda as cyber operations can be done remotely and are comparatively safer than strapping on a bomb.<sup>76</sup> A British Home Office report recently noted that “[s]ince the death of Osama bin Laden, al-Qaeda has explicitly called not only for acts of lone or individual terrorism but for ‘cyber jihad.’”<sup>77</sup>

### III. COUNTERING NEW TECHNOLOGY WITH TECHNOLOGY

The aggressive pursuit of new technology by non-state armed groups clearly poses long-term humanitarian risks. However, of greater immediate humanitarian concern are the evolving mitigation methods, or tactics, used by non-state armed groups to counter the technological superiority of state actors. Increasingly adept at communicating, organizing, and operating from any location, non-state armed groups are less and less tied to “hot battlefields,”<sup>78</sup> and are more likely to shield their operations by deeply embedding within unsuspecting local populations across the world.<sup>79</sup> Additionally, technology, and

<sup>75</sup> See QDR, *supra* note 6, at 37.

<sup>76</sup> *ABC Nightly News: Former CIA Counter-Terror Chief: Al Qaeda Will Go Cyber*, (ABC television broadcast Aug. 4, 2011), available at <http://abcnews.go.com/Blotter/cia-counter-terror-chief-al-qaeda-cyber/story?id=14224256>.

<sup>77</sup> Duncan Gardham, *Terrorists Are Harnessing Hi-tech Communications, Government Warns*, THE TELEGRAPH (July 12, 2011, 7:18 PM), <http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8633311/Terrorists-are-harnessing-hi-tech-communications-government-warns.html>.

<sup>78</sup> “Hot battlefields” is a term used to reference geographically contained conflicts. For example, Afghanistan, or until recently, Iraq would be construed as a “hot battlefield.” See, e.g., Ashley S. Deeks, *Pakistan's Sovereignty and The Killing of Osama Bin Laden*, AMERICAN SOCIETY OF INTERNATIONAL LAW INSIGHTS (MAY 5, 2011), <http://www.asil.org/insights110505.cfm> (“[T]he most controversial aspect . . . is the U.S. argument that this conflict can and does extend beyond the “hot battlefield” of Afghanistan to wherever members of al Qaeda are found.”); Margaret Talev, *U.S. to Attack Al-Qaeda Terrorists Beyond the ‘Hot Battlefields,’ Brennan Says*, BLOOMBERG (Sept. 16, 2001), <http://www.bloomberg.com/news/2011-09-16/u-s-will-hit-al-qaeda-beyond-hot-battlefields-obama-aide-brennan-says.html> (discussing the use of military force against Al-Qaeda away from “hot battlefields” like Afghanistan).

<sup>79</sup> The illegality of using civilians as a “shield” is without question in international armed conflicts. See AP I, *supra* note 11, at art. 51(7) (“the civilian population or individual civilians shall not be used to render certain points or areas immune from military operations, in particular in attempts to shield military objectives from attacks or to shield, favour or impede military operation.”); See also Geneva Convention Relative to the Protection of Civilian Persons in Time of War, art. 28, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 (“The presence of a protected person may not be used to render certain points or areas immune from military operations”); Rome Statute of the International Criminal Court art 8(2)(b)(xxiii), July 17, 1998, 37 I.L.M. 1002, 2187 U.N.T.S. 90 (listing as a war crime “[u]tilizing the presence of a civilian or other protected person to render certain points, areas or military forces immune from military

in particular cyber technology, now allows for these groups to conduct asymmetric activities with fewer risks and minimal resources thus further cloaking their existence. Broadly dispersed and quietly blended into various civilian population centers, state actor advantages are mitigated as the non-state actor is virtually indistinguishable from a civilian.<sup>80</sup> This pervasive exploitation of civilians, and the intentional assault on the principle of distinction, threatens the delicate balance between military necessity and humanity undercuts the paramount purpose of the Law of War.<sup>81</sup>

In general terms, non-state armed groups cannot survive direct and conventional conflicts with more technologically superior state opponents.<sup>82</sup> To compete, these groups consciously “avoid mirroring Western military organizations and approaches to war”<sup>83</sup> and “by operating well outside the moral framework of the traditional Western approach” to hostilities.<sup>84</sup> Unconstrained by these assumed “universal norms of behaviour”<sup>85</sup> non-state armed groups can seek advantages by practicing unorthodox, or even legally prohibited, approaches to warfare. The Law of War mandate requiring parties to a conflict to distinguish between civilians and conflict participants<sup>86</sup> is

---

operations.”). Though not as clearly articulated, the prohibition on misusing civilians also exists in non-international armed conflicts. See Protocol Additional to the Geneva Conventions of August 1949, and Relating to the Protection of Victims of Non-International Armed Conflict (Protocol II) art. 13, June 8, 1977, 1125 U.N.T.S. 609 [hereinafter AP II] (discussing general protections for civilians in non-international armed conflicts); GARY SOLIS, *THE LAW OF ARMED CONFLICT: INTERNATIONAL HUMANITARIAN LAW IN WAR* 100-01(2010) (“[W]ar crimes and grave breaches can indeed be committed in non-international common Article 3 armed conflicts.”).

<sup>80</sup> Nils Melzer, *Foreword to Keeping the Balance Between Military Necessity and Humanity: A Response to Four Critiques of the ICRC’s Interpretive Guidance on the Notion of Direct Participation in Hostilities*, 42 N.Y.U. J. INT’L L. & POL. 831, 833 (2010) (discussing the difficulties in contemporary armed conflicts due to the “blurring of the traditional distinctions and categories upon which the normative edifice of IHL has been built. . .”).

<sup>81</sup> See Nils Melzer, *Foreword to Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law* 4, ICRC (May 2009) [hereinafter ICRC Interpretive Guidance], available at <http://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf> (stating that “the protection of civilians is one of the main goals of international humanitarian law.”).

<sup>82</sup> See generally McKenzie Jr., *supra* note 3.

<sup>83</sup> See *infra* Section II for discussion on the various approaches to warfare adopted by contemporary non-state armed groups.

<sup>84</sup> McKenzie Jr., *supra* note 3, at 88.

<sup>85</sup> *Id.*

<sup>86</sup> See AP I, *supra* note 11, art. 48. The distinction requirement also applies in non-international armed conflict. See AP II, *supra* note 82, art. 13 (stating “[c]ivilians shall enjoy the protection afforded by this part, unless and for such time as they take a direct part in hostilities”); See also SOLIS, *supra* note 82, at 254 (discussing the applicability of the principle of distinction in all conflicts); Cf Kenneth Watkin, *Opportunity Lost: Organized Armed Groups and the ICRC “Direct Participation in Hostilities” Interpretive Guidance*, 42 N.Y.U. J. INT’L L. & POL. 641, 646 (2010)

therefore an opportunity for the non-state armed group versus an obligation for the state actor.<sup>87</sup> Whereas the state actor must protect civilians, the non-state armed group simply views civilians as an asymmetric warfare asset that may be leveraged in order to gain an advantage against their state actor adversaries.<sup>88</sup>

Considering civilians as an “asset to be expended”<sup>89</sup> non-state armed groups blatantly ignore the general protections afforded non-combatants during hostilities.<sup>90</sup> Yet this callous disregard for long-standing humanitarian norms<sup>91</sup> is sadly not unusual or surprising. Despite the international impetus to protect civilians from the atrocities of war,<sup>92</sup> the state actor’s resultant legal obligations perversely incentivises non-state actors to misuse civilians. Contemporary conflicts “waged between government forces and organized non-state armed groups” are routinely characterized by an “intermingling of civilians and armed actors” and a stubborn unwillingness of non-state actors to “adequately distinguish themselves from the civilian population.”<sup>93</sup> As these conflicts are now the predominant form of warfare<sup>94</sup> this intentional misuse of civilians by non-state armed groups is a harsh reality driving a number of responses from state actors.

Though often perceived as “fighting with one arm tied behind [their] back” and admittedly causing much frustration, state actors recognize the importance of complying with the Law of War as “preserving the rule of law. . . constitutes an important component of [their] security stance.”<sup>95</sup> State actors thus

---

(“[c]ompliance with the distinction principle is required of all participants in warfare regardless of whether they fight for state armed forces or a non-State ‘organized armed group.’”).

<sup>87</sup> See SOLIS, *supra* note 82, at 254 (discussing the frequent disregard for the principle of distinction by non-state actors).

<sup>88</sup> See generally McKenzie Jr., *supra* note 3, at 76.

<sup>89</sup> *Id.* at 88.

<sup>90</sup> See, e.g., Laura King, *Afghanistan Arrests Preteen Would-be Bombers Months After Pardon*, LOS ANGELES TIMES, (Feb. 13, 2012), <http://www.latimes.com/news/nationworld/world/la-fg-afghanistan-child-bombers-20120214,0,7784954.story> (last visited Feb. 17, 2012) (describing how insurgents in Afghanistan are using young children as suicide bombers).

<sup>91</sup> See, COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUG. 1949, 598 (Yves Sandoz, et. al. eds., 1987) [hereinafter Commentaries] (“It is the foundation on which the codification of the laws and customs of war rests: the civilian population and civilian objects must be respected and protected . . . . The entire system established in The Hague in 1899 and 1907 and in Geneva from 1864 to 1977 is founded on this rule.”).

<sup>92</sup> See *Id.* (discussing the historical reason for protecting civilians and the particular need for a codification of this customary understanding following the brutality of World War II).

<sup>93</sup> ICRC Interpretive Guidance, *supra* note 84, at 4–5.

<sup>94</sup> See Watkin, *supra* note 89, at 653.

<sup>95</sup> *Id.* at 647 (citing HCJ 769/02 Pub. Comm. Against Torture in Israel v. Gov’t of Israel 64 [2005] (Isr.), available at [http://elyon1.court.gov.il/files\\_eng/02/690/007/a34/02007690.a34.pdf](http://elyon1.court.gov.il/files_eng/02/690/007/a34/02007690.a34.pdf)

“operate under constraints when conducting operations,” and in particular strive to comply with the distinction principle in these complex and messy conflicts.<sup>96</sup> Using a combination of policy mandates and advanced technology, state actors continually try to disentangle non-state actors from local populations. For example, the United States military, desperate to reduce civilian casualties in the often confusing environments of Iraq and Afghanistan, has universally implemented the Escalation of Force (EOF) process.<sup>97</sup> The EOF process trains American soldiers to work through a number of sequential steps in order to distinguish between a harmless civilian and an actual threat in hopes of gaining clarity before using deadly force.<sup>98</sup> Similarly, The North Atlantic Treaty Organization’s (NATO) 6 July 2009 Tactical Directive imposed restrictions on a number of weapon systems and tactics in hopes of reducing civilian casualties in Afghanistan.<sup>99</sup>

State actors also rely heavily on technology to help determine who can be targeted.<sup>100</sup> The United States uses a scientific, heavily computerized, deliberate targeting process known as the Collateral Damage Estimation,<sup>101</sup> to ensure strict compliance with both the distinction and proportionality principles.<sup>102</sup> Non-lethal Unmanned Aerial Vehicles (UAV) are a common tool of government forces to help pierce the “fog of war” and decipher the intentions of individual actors in a conflict zone.<sup>103</sup> Precision-guided munitions allow for

---

(discussing pragmatic security reasons that a state will self-restrain their combat activities).

<sup>96</sup> *Id.* at 64–67.

<sup>97</sup> See generally Randall Bagwell, *The Threat Assessment Process (TAP): The Evolution of Escalation of Force*, ARMY LAW., Apr. 2008, at 5.

<sup>98</sup> *Id.* at 8 (“The goal . . . is to force the insurgent to self-identify while keeping innocent civilians from being mistaken for threats. This approach works primarily because it uses non-force measures to put potential threats into situations where they must either comply with or disobey the Soldiers’ commands.”).

<sup>99</sup> See Headquarters, Int’l Sec. Assistance Force, Tactical Dir. (July 6, 2009) [hereinafter Tactical Directive], available at [http://www.nato.int/isaf/docu/official\\_texts/Tactical\\_Directive\\_090706.pdf](http://www.nato.int/isaf/docu/official_texts/Tactical_Directive_090706.pdf).

<sup>100</sup> Watkin, *supra* note 89, at 646 (“At the heart of the question of who can be targeted is the principle of distinction.”).

<sup>101</sup> See generally Gregory S. McNeal, *The U.S. Practice of Collateral Damage Estimation and Mitigation* (Nov. 9, 2011) (Unpublished Working Paper) (discussing the technical methodology employed by the United States for pre-planned targeting and its overarching goal of minimizing civilian casualties) available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1819583](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1819583).

<sup>102</sup> The Principle of Proportionality determines whether “an attack . . . may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof [that will] be excessive in relation to the concrete and direct military advantage anticipated.” AP I, *supra* note 11, at art. 51(5)(b).

<sup>103</sup> See Martin E. Dempsey, *Forward* to U.S. Army UAS Ctr. Of Excellence, “Eyes of the Army” U.S. Army Unmanned Aircraft Systems Roadmap 2010-2035, U.S. ARMY, i (2010), <http://www-rucker.army.mil/usaace/uas/US%20Army%20UAS%20RoadMap%202010%202035.pdf>

extraordinarily accurate and discriminate targeting<sup>104</sup> while electronic intelligence gathering pinpoints clandestine non-state actors. Yet, despite these policy restrictions and technological advances, complying with the principle of distinction remains extraordinarily difficult for state actors<sup>105</sup> as “the principle . . . is easy to state” but challenging to implement.<sup>106</sup>

Implementation challenges are largely a result of the realities of contemporary conflicts. As non-state armed groups intentionally mix with civilians, the task of discerning an individual's status and their accompanying level of humanitarian protection<sup>107</sup> often falls to junior leaders and their soldiers.<sup>108</sup> Further, non-state armed groups are not passively using the civilian population as a shield from attack, but, in furtherance of their asymmetric strategy, will often attempt to draw a disproportionate response from the state actor in order to further a propaganda message.<sup>109</sup> Practical implementation of the principle of distinction in day-to-day operations therefore becomes the responsibility of the “soldiers and other fighters.”<sup>110</sup> The enormity of this responsibility coupled with the complexity of the modern battlefield understandably leads to “confusion and uncertainty as to the distinction between legitimate military targets and persons protected against direct

---

(stating that unmanned aerial vehicles help to “broaden situational awareness” as well as improve the ability to “see, target, and destroy the enemy” in uncertain and complex environments).

<sup>104</sup> See, e.g., *Al-Qaeda's Anwar al-Awlaki killed in Yemen*, CBS NEWS (Sept. 30, 2011, 5:02 AM), <http://www.cbsnews.com/stories/2011/09/30/501364/main20113732.shtml>.

<sup>105</sup> See Melzer, *supra* note 83, at 833 (noting that the increased civilian involvement in modern warfare has led distinction problems between legitimate military targets and persons protected against direct attack.”).

<sup>106</sup> Watkin, *supra* note 89, at 646.

<sup>107</sup> See SOLIS, *supra* note 82, at 187 (“On the battlefield, no one is without some status and an accompanying level of humanitarian protection.”).

<sup>108</sup> See Charles C. Krulak, *The Strategic Corporal: Leadership in the Three Block War*, MARINES MAG. Jan. 1999, at 26, 30 (1999), available at [http://www.au.af.mil/au/awc/awcgate/usmc/strategic\\_corporal.htm](http://www.au.af.mil/au/awc/awcgate/usmc/strategic_corporal.htm) (stating the strategic corporal concept is a recognition that modern conflicts will see “the lines separating the levels of war, and distinguishing combatant from ‘non-combatant,’” blur and “and adversaries, confounded by . . . [the state’s] ‘conventional’ superiority, will resort to asymmetrical means to redress the imbalance.” As a result, the success of the modern battlefield will “rest, increasingly, with the rifleman and with his ability to make the *right* decision at the *right* time at the point of contact.”).

<sup>109</sup> See U.S. DEP’T OF ARMY, FM 3-24, *supra* note 5, at ¶ 1–152 (stating that non-state armed groups will “carry out a terrorist act or guerrilla raid” with the primary purpose of enticing the opposing actor “to overreact” in a way that can be exploited “—for example, opening fire on a crowd . . . .”); McKenzie Jr., *supra* note 3, at 77 (discussing how “asymmetric approaches can achieve powerful effect through manipulation of the psychological element.”).

<sup>110</sup> Watkin, *supra* note 89, at 646.

attack.”<sup>111</sup>

This “confusion and uncertainty” is a hallmark of the state actor conflict with the non-state armed group and creates significant humanitarian risks for civilian populations.<sup>112</sup> It is therefore particularly alarming that non-state armed groups are further complicating these conflicts by using advanced technology, and specifically information technology, to expand their operations across the entirety of the international community. Widely dispersed, yet capable of operating and collaborating through cyberspace, non-state armed groups are extensively transnational.<sup>113</sup> Further, the cyber domain allows for more discrete forms of terror activities with the contemporary non-state actor more likely to be a financier, strategic planner, or propagandist than a “traditional terrorist” operator.<sup>114</sup> A non-exhaustive list of examples includes: Anwar al-Awlaki, from a remote location in Yemen, encouraging and coordinating various terror operations, particularly in the United States, by using “Youtube, broader Internet sites, Facebook, [and] Twitter;”<sup>115</sup> al-Qaeda computer operatives widely publishing versions of bomb-making manuals, often in English, on the Internet to encourage remote training;<sup>116</sup> groups such

---

<sup>111</sup> Melzer, *supra* note 83, at 833.

<sup>112</sup> See, e.g., Goldstone Report, *supra* note 12 (alleging a number of Law of War violations that involved civilians committed by both Israeli forces and Hamas during the conflict in Gaza from 27 December 2008 to 18 January 2009); but see State of Israel, *Gaza Operations Investigations: An Update* 32 (Jan. 2010), <http://www.mfa.gov.il/NR/rdonlyres/8E841A98-1755-413DA1D2-8B30F64022BE/0/GazaOperationInvestigationsUpdate.pdf> (refuting the Goldstone Reports findings); See also Kevin Sieff, *Afghan Civilian Deaths Hit Record High in 2011*, U.N. Report Says, WASH. POST, Feb. 4, 2012 [http://www.washingtonpost.com/world/afghan-civilian-deaths-hit-record-high-in-2011-un-report-says/2012/02/04/gIQAfYl9oQ\\_story.html](http://www.washingtonpost.com/world/afghan-civilian-deaths-hit-record-high-in-2011-un-report-says/2012/02/04/gIQAfYl9oQ_story.html) (noting that the vast majority of the civilian deaths came from Taliban roadside or suicide bombings).

<sup>113</sup> See RUSSELL D. HOWARD & REID L. SAWYER, *TERRORISM AND COUNTERTERRORISM—UNDERSTANDING THE NEW SECURITY ENVIRONMENT* 77 (2004) (noting that al-Qaeda is a global network consisting of permanent or independently operating semi-permanent cells of trained militants that have a presence in more than seventy-six countries).

<sup>114</sup> See, e.g., Brian Ross, *How Anwar al-Awlaki Inspired Terror From Across the Globe*, ABC NEWS THE BLOTTER <http://abcnews.go.com/Blotter/anwar-al-awlaki-inspired-terror/story?id=14643383> (describing al-Awlaki as the “modern day terrorist” capable of using the internet to conduct terrorist activity).

<sup>115</sup> *Id.* (“While al-Awlaki was not the trigger-man in any of the 19 terror operations to which he is linked, U.S. officials and terror experts said that his hand was visible in all of them—whether by simply pushing the attackers over the violent edge or by personally guiding them through operations.”).

<sup>116</sup> See Duncan Gardham, *Al-Qaeda Bomb Manual Published on Internet*, THE TELEGRAPH, (Feb. 22, 2012, 7:00 AM), <http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8232389/Al-Qaeda-bomb-manual-published-on-internet.html> (“Published by al-Qaeda’s Global Islamic Media Front” in order allow followers “to launch their own attacks, without training.”).

asal-Qaeda, Hamas, Lashkare-Taiba, and Hezbollah, "mak[ing] extensive use of the Internet to raise and transfer needed funds to support their activities" as the Internet "offers a broad reach, timely efficiency, as well as a certain degree of anonymity and security for both donors and recipients."<sup>117</sup> These types of activities make the non-state actor not only exceedingly difficult to identify, these actions also make the global population, even if ignorant about the hostilities, potentially a de facto human shield. This trend towards decentralized, discrete non-state actor terrorist activity thus further blurs the lines drawn within the principle of distinction between conflict participant and civilian while dramatically increasing the civilian population's exposure to hostilities.

State actors are simply not prepared for this trend. Previous responses, whether policy mandates or sophisticated technology, relied upon to clarify individual status on the modern battlefield are of minimal use in these transnational conflicts. Rules of engagement, tactical directives, and soldier training are almost exclusively oriented on non-international conflicts within a specific geographic area.<sup>118</sup> Sophisticated technology is limited by resources and intelligence and thus difficult to employ without some parameters. These shortcomings ensure that non-state armed groups will continue to counter the technological superiority of state actors by exploiting the distinction principle. This leaves state actors and the international community again left with the seemingly impossible task of determining "how . . . the principle of distinction should be implemented in the challenging and complex circumstances of contemporary warfare."<sup>119</sup> This has become a contentious, and difficult to answer question.<sup>120</sup> But without an answer, the walls separating combatant and civilian will continue to crumble, creating the very real, and dangerous, possibility that warfare will again degenerate "into brutality and savagery."<sup>121</sup>

---

<sup>117</sup> Michael Jacobson, *Terrorist Financing and the Internet*, 33 *STUD. IN CONFLICT AND TERRORISM* 353 (2010).

<sup>118</sup> See, e.g., Tactical Directive, *supra* note 102 (restricting NATO operations in Afghanistan).

<sup>119</sup> MELZNER, *supra* note 84, at 7.

<sup>120</sup> Compare MELZNER, *supra* note 84 (providing recommendations on how to implement the principle of distinction) with Watkin, *supra* note 89, and Michael N. Schmitt, *The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis*, 1 *HARV. NAT. SEC. J.* 1, 5 (May 2010) (criticizing the Interpretive Guidance recommendations).

<sup>121</sup> Rob McLaughlin, *The Law of Armed Conflict and International Human Rights Law: Some Paradigmatic Differences and Operational Implications*, 2010 *Y.B. OF INT'L HUM. L.* 213, 222 (citing United Kingdom Ministry of Defence, *The Manual on the Law of Armed Conflict*, 2004, ¶ 1.8.).



## IV. CONCLUSION

The relationship between non-state armed groups and advanced technology creates a number of uncertain and frightening humanitarian challenges for the international community. The “widespread availability of sophisticated weapons and equipment . . . ‘level the playing field’ and negate [state actor’s] traditional technological superiority”<sup>122</sup> while exponentially increasing the lethality of the non-state armed group. Unrestrained by law or morality, non-state armed groups’ growing familiarity with unmanned aerial vehicles, weapons of mass destruction, surface-to-air missiles, information technology, and improvised explosive devices is extraordinarily dangerous. Similarly, while mitigating state actor technological superiority by commingling with civilians is not a new tactic,<sup>123</sup> advanced technology is allowing non-state armed groups to expand this tactic across the globe at an unprecedented rate.<sup>124</sup> Capable of supporting operations with seemingly benign activity, these widely dispersed non-state actors are difficult to identify and place previously safe civilian populations at risk. Additionally, this increased ability to use advanced technology to aggressively exploit the state obligation to distinguish between civilians and conflict participants de-legitimizes and undercuts this fundamental principle of the Law of War.

The necessity for the international community to recognize and address these ominous threats is clear. The humanitarian consequences of inaction place untold civilians at risk while raising troubling questions concerning the effectiveness of the Law of War to regulate contemporary conflicts. Facing “a complex and uncertain security landscape in which the pace of change continues to accelerate,”<sup>125</sup> the international community must adapt to this new reality and redouble previous efforts to stop this potential humanitarian crisis.



---

<sup>122</sup> Krulak, *supra* note 111.

<sup>123</sup> Ryan Goodman & Derek Jinks, *The ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law: An Introduction to the Forum*, 42 N.Y.U. J. INT’L L. & POL. 637, 637 (2010) (“the most intractable conflicts now include non-state armed groups that wear no uniform and purposefully commingle their fighters with civilian populations.”).

<sup>124</sup> *Id.* (“Technological developments have expanded the capacity of individuals to apply lethal force while remaining located thousands of miles away from their targets.”).

<sup>125</sup> QDR, *supra* note 6, at p. iii.

## ARTICLE

### Sun Tzu's Battle For Your Footnotes: The Emergent Role Of Libraries In Juridical Warfare

Mark McCary<sup>\*</sup>

A wise general makes a point of foraging on the enemy.  
—Sun Tzu, *The Art of War*, Waging War<sup>1</sup>

#### ABSTRACT

*This paper posits that libraries—specifically science and technology libraries—have emerged on the international scene as a critical source of soft power—non-military power.<sup>2</sup> Public and private entities can leverage a library's digital resources to accelerate<sup>3</sup> the development of critical technologies<sup>4</sup>*

---

<sup>\*</sup> Attorney, Texas License, 2000; Robert Bosch Foundation Fellow, 2000–2001; J.D., University of Texas at Austin, 1999; B.A., Virginia Military Institute, 1992. Major, U.S.A.F.R., 1992–Present. McCary & McCary, P.C., <http://www.m2lawpc.com>. Dedicated to those serving in Academia. (Assessments are based on the Author's personal defense related experience and renewables industry related work. Views are not necessarily representative of U.S. Government policy positions.)

<sup>1</sup> SUN TZU, *THE ART OF WAR* 14 (James Clavell, ed., Delta 1988) (6th Cent. B.C.); see also *id.* at 9 (“The Art of War is of vital importance to the state. It is a matter of life and death, a road either to safety or to ruin. Hence under no circumstances can it be neglected.”).

<sup>2</sup> See JOSEPH S. NYE, JR., *SOFT POWER: THE MEANS TO SUCCESS IN WORLD POLITICS* 76–77 (2004) (noting research in physics and chemistry, internet websites, patents, and R&D expenditures as potential means of soft power); see also *id.* at 83–85 (discussing Asian power and stating that it will take some time for China to have the same soft power impact the U.S. enjoys).

<sup>3</sup> See David Kramer, *Science Board Details China's Leap in Science and Technology*, *PHYSICS TODAY*, Mar. 2010, at 30 (“If anyone still needs convincing on the speed with which China is ascending as a world science and technology (S&T) leader, the latest edition of *Science and Engineering Indicators*, the biennial encyclopedia of statistics assembled by the National Science Board (NSB) should suffice.”); see also *id.* at 30 (noting that China's research workforce has nearly tripled from 500,000 in 1995 to nearly 1.4 million in 2007 and its emphasis on investment and education has achieved a dramatic amount of synergy).

<sup>4</sup> From the author's perspective, science and technology libraries provide access to baseline research necessary to accelerating innovation by shorting the time necessary to prepare or accumulate experimental and theoretical knowledge required for technological advancement. Cf. S.J. DEITCHMAN, *BEYOND THE THAW: A NEW NATIONAL STRATEGY* 193–211 (1991) (discussing aspects of accelerated technology development and arguing there is a need to maintain the edge in such areas as computing hardware and software, materials, aircraft and missiles, fiber optics, superconductivity, directed energy, etc., and noting that if we lose a lead we may never regain it as we face an increasingly uncertain future and pointing out that

*through horizon scanning,<sup>5</sup> targeting,<sup>6</sup> early warning<sup>7</sup>, alert services<sup>8</sup>, digital exploitation,<sup>9</sup> and cross-domain delivery.<sup>10</sup> Library resources play a key role in strengthening the research capabilities of public and private entities. However, current library trends threaten cutting-edge proprietary research intended for only very private audiences.*

---

focusing on civilian technology advancements can pay dividends for military defense strategy).

<sup>5</sup> Horizon Scanning is defined by the author as the electronic survey of available digital information resources, including blogs, social networks, search engines, portals, newsgroups, intranets, to deliver the proper information to the proper customer at the proper time. It is generally accomplished through the use of software tools. See, e.g., Horizon Scanning, AMI ENTERPRISE INTELLIGENCE SOFTWARE, <http://www.amisw.co.uk/horizon-scanning-solution.html> (last visited Jan. 4, 2012) (defining horizon scanning and offering for sale horizon scanning software).

<sup>6</sup> Targeting is defined by the author as those activities designed to identify and exploit a research and development objective. Military concepts of reconnaissance, surveillance, target identification, and selection have been translated into Competitive Intelligence theories and practices. See JOINT CHIEFS OF STAFF, JOINT PUBLICATION 3-60: JOINT DOCTRINE FOR TARGETING (2007) [http://www.bits.de/NRANEU/others/jp-doctrine/jp3\\_60\(02\).pdf](http://www.bits.de/NRANEU/others/jp-doctrine/jp3_60(02).pdf) (discussing the definition, nature, and characteristics of targets and the joint targeting process); U.S. AIR FORCE, AIR FORCE DOCTRINE DOCUMENT 2-1.9: TARGETING (2006), <http://www.fas.org/irp/dodd%20ir/usaf/afdd2-1.9.pdf> (establishing "doctrinal guidance for planning, executing, and assessing targeting operations"); U.S. AIR FORCE, AIR FORCE INSTRUCTION 14-117: AIR FORCE TARGETING (2009) <http://www.af.mil/shared/media/epubs/AFI14-117.pdf> (defining Air Force targeting responsibilities).

<sup>7</sup> *Early Warning* is defined by the author as a system of analysis used to timely determine risks, market shifts, and competitor developments in a particular industry. This system of analysis is augmented by sophisticated software tools that provide web surveillance and reconnaissance. See, e.g., *ICI-32 - Early Warning Systems*, INSTITUTE FOR COMPETITIVE INTELLIGENCE, [http://competitiveintelligence.ning.com/events/ici32 early warning systems 2](http://competitiveintelligence.ning.com/events/ici32%20early%20warning%20systems) (last visited Jan. 4, 2012) (discussing the fundamentals for the design of early detection and warning systems); see also Adrian Alvarez, *Situational Early Warning*, COMPETITIVE INTELLIGENCE MAG., Jan.–Feb. 2007, at 14–18 (discussing the key steps in situational early warning methodology).

<sup>8</sup> Alert Services are defined by the author as those means used to alert customers to breaking competitive intelligence developments. Alert Services are often combined with Horizon Scanning and Early Warning although each is distinct in nature. See, e.g., CyberAlert Applications, CYBER ALERT, [http://www.cyberalert.com/app\\_competitive\\_intelligence.html](http://www.cyberalert.com/app_competitive_intelligence.html) (last visited Jan. 4, 2012) (describing competitive intelligence services offered for purchase).

<sup>9</sup> Digital Exploitation is defined by the author as those means used to take unfair advantage of a competitor's digitized pre-competitive data.

<sup>10</sup> Cross-Domain Delivery is defined as the assembly of critical technology information from various disciplines that are ultimately associated with one technological innovation for use by a consumer—e.g. stealth technology; Cf. Feeding the Dragon: Technology Transfer and the Growing Chinese Threat Before the Joint Economic Committee, 105th Cong. (1997) (statement of Peter M. Leitner), available at [www.house.gov/jec/hearings/espionag/leitner.htm](http://www.house.gov/jec/hearings/espionag/leitner.htm) (discussing integration of technologies and forecasting a projected loss of technology edge to future adversaries such as China, specifically in the field of stealth technology).

*Western authors, who submit for early circulation publications on emerging technology issues, may find their works exploited through deep dive research,<sup>11</sup> citation analysis, unsanctioned access, and networked digital library ("DL") holdings. Separately, Western librarians may find themselves victims of information attack via surreptitious inquiries for unclassified but sensitive materials or cyber penetrations.<sup>12</sup> The end result can be a hostile competitor's reliance on library information systems for unauthorized and competitive development of dual-use (civilian/military) applications.<sup>13</sup> More importantly, these library trends can be used to undercut the legal precepts of newness and innovation necessary to patent law.<sup>14</sup>*

*This paper draws on China as a case study to help lawyers, businessmen, researchers, and analysts better understand threats and defensive strategies for intellectual property rights. China provides an example of how a competitor state, also characterized as a peer adversary,<sup>15</sup> relies on its National Science Library ("NSL") and Competitive Intelligence strategy to boost research advantage for State-influenced academic, governmental, and military entities.<sup>16</sup> China's LIS marshals soft power through tactical and strategic intelligence collection/analysis,<sup>17</sup> early warning and alert services,<sup>18</sup> and regulatory/patent*

---

<sup>11</sup> Deep Dive Research is defined by the author as any research activity that goes beyond first-line web searches.

<sup>12</sup> See Joanne Kuzma, European Digital Libraries—Web Security Vulnerabilities, 28 LIBRARY HI TECH 402, 402–13 (2010) (discussing "[s]ecurity problems and breaches" and noting that librarians have "unique security concerns compared to other industries").

<sup>13</sup> See DEITCHMAN, *supra* note 5, at 193 (defining "dual-use" as advances in materials and electronics that have application in both the military and civilian spheres and which are fundamentally important to both spheres).

<sup>14</sup> See e.g., ARTHUR R. MILLER & MICHAEL H. DAVIS, INTELLECTUAL PROPERTY—PATENTS, TRADEMARKS, AND COPYRIGHT—IN A NUTSHELL 40–66 (2007) (providing a basic overview of the patent law principal of novelty).

<sup>15</sup> Martin C. Libicki, The Next Enemy, STRATEGIC FORUM, Jul. 1995, at 1, 1–2, <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA394657> (discussing China as an emergent peer adversary and highlighting future competition in the field of information warfare).

<sup>16</sup> See Zhang Zuozhi George, Competitive Intelligence Development in China, COMPETITIVE INTELLIGENCE MAG., Nov.–Dec. 2008, at 6–11, available at <http://www.scip.org/Publications/CIMArticleDetail.cfm> (discussing China's developing emphasis on Competitive Intelligence (CI) theories at all levels and specifically noting incorporation of CI programs into academic settings); see also Xinzhou Xie & Xuehui Jin, The Evolution of Competitive Intelligence in China, 1 J. OF INTELLIGENCE STUD. IN BUS. 61–75 (2011) (providing a critical overview of the evolution of CI in China).

<sup>17</sup> See generally Jinxia Huang, Presentation: Information Development & Knowledge Services in National Science Library, The Chinese Academy of Sciences, CORNELL UNIV. LIBR. STAFFWEB (Mar. 15, 2010), [http://staffweb.library.cornell.edu/system/files/ChineseAcademyofSciences\\_JinxiaHuan\\_g\\_March2010\\_0.pptx](http://staffweb.library.cornell.edu/system/files/ChineseAcademyofSciences_JinxiaHuan_g_March2010_0.pptx) (providing background information on the Chinese National Science

lawfare.<sup>19</sup> In doing so, China's LIS is positioned as a force multiplier.<sup>20</sup> It serves as a science and technology-targeting platform<sup>21</sup> to accelerate development of national technology objectives.<sup>22</sup> Ultimately, China's LIS promotes rapidity and surprise in warfare that has no rules.<sup>23</sup> It is a perfectly designed strategic tool for maintaining the technological upper hand amidst the U.S. policy of integration.<sup>24</sup>

## Table of Contents

---

I. PROLOGUE.....	50
II. THE BATTLE SPACE.....	51
III. JURIDICAL WARFARE STRATEGY.....	53
IV. THE EMERGING LIBRARY MODEL— SCIENCE AND TECHNOLOGY TARGETING CENTERS.....	57
V. THE TARGET—NEWNESS AND INNOVATION.....	61
VI. A HYPOTHETICAL.....	62
VII. THE PROOF.....	63

---

Library and the way that library researchers conduct information analysis).

<sup>18</sup> *Id.*

<sup>19</sup> *Id.*

<sup>20</sup> See generally Dale G. Uhler, *Technology—Force Multiplier for Special Operations*, JOINT FORCES Q., 1st QTR 2006, at 54, [http://www.dtic.mil/doctrine/jel/jfq\\_pubs/4012.pdf](http://www.dtic.mil/doctrine/jel/jfq_pubs/4012.pdf) (discussing generally technology as a force multiplier). In similar vein, libraries provide the platform for which new technologies can be developed. The generally accepted Department of Defense definition for “force multiplier” is “[a] capability that, when added to and employed by a combat force, significantly increases the combat potential of that force.” *Force Multiplier Definition*, DOD DICTIONARY OF MILITARY TERMS, [http://www.dtic.mil/doctrine/dod\\_dictionary/?zoom\\_query=FORCE+MULTIPLIER&zoom\\_sort=0&zoom\\_per\\_page=10&zoom\\_and=1](http://www.dtic.mil/doctrine/dod_dictionary/?zoom_query=FORCE+MULTIPLIER&zoom_sort=0&zoom_per_page=10&zoom_and=1) (last visited Jan. 4, 2012).

<sup>21</sup> Cf. AIR FORCE INSTRUCTION 14-117, *supra* note 7 (discussing targeting).

<sup>22</sup> See Liu Xiwen, *Presentation: Policy-Making Oriented Information Services of Scientific and Technological Libraries in China*, TEKNILLINEN KORKEAKOULU (June 18, 2008), [http://lib.tkk.fi/ifa/IFLA\\_Science\\_Portals/Presentations/Liuxw.pdf](http://lib.tkk.fi/ifa/IFLA_Science_Portals/Presentations/Liuxw.pdf) (discussing science and technology services of the National Science library, which include analysis of science and technology documents, scientific data and scientific data intelligence, intelligence analysis of science and technology strategy, monitoring of science and technology development trends, and provision of alert services related to certain science and technology fields).

<sup>23</sup> See QIAO LIANG & WANG XIANGSUI, UNRESTRICTED WARFARE 28–32 (Pan Am. Publ'g Co. 2002) (1999) (discussing various strata of the battlespace).

<sup>24</sup> U.S. policy is to fully integrate China into the global rules based economic and trading system and expand exports into Chinese markets in spite of China's advocacy of legal and economic warfare. See *Background Note: China*, U.S. DEPT. OF STATE, [www.state.gov/r/pa/ei/bgn/18902.htm](http://www.state.gov/r/pa/ei/bgn/18902.htm) (last updated Sept. 6, 2011) (discussing the U.S. approach to relations with China).

VIII.	COMPETITOR COLLECTORS.....	64
IX.	COLLECTION STRATEGY.....	66
X.	MOTIVATION AND DRIVE.....	67
XI.	COMPETITIVE INTELLIGENCE MISSION.....	68
XII.	DIGITAL EXPLOITATION.....	68
XIII.	OFFENSIVE RESEARCH TECHNIQUES.....	69
XIV.	E-LIBRARY TARGETING TOOLS.....	71
XV.	CHINESE LIBRARIANS—BIBLIO WARFARE SPECIALISTS.....	75
XVI.	THE OYSTER EFFECT.....	77
XVII.	ARCHITECTURE OF CHINA'S NATIONAL SCIENCE LIBRARY.....	78
XVIII.	NATIONAL DIRECTION.....	81
XIX.	CULTURED PEARLS.....	83
XX.	CHAIN OF COMMAND.....	85
XXI.	ORGANIZATIONAL STRUCTURE.....	86
XXII.	OPERATING AREA.....	90
XXIII.	PREDATION.....	92
XXIV.	SITUATIONAL AWARENESS.....	93
XXV.	RULE OF CAPTURE.....	94
XXVI.	RETRENCHMENT.....	95
XXVII.	THE VULNERABILITY.....	96
XXVIII.	IMPACT.....	100
XXIX.	EPILOGUE.....	102
	APPENDICES I-XIII. ....	103

## I. PROLOGUE

The purpose of this paper is threefold: (1) to stimulate primary collection on the future role of science and technology libraries in pre-competitive research and patent developments; (2) to advise Western researchers that the Chinese National Science Library (NSL) is targeting advanced technology sectors for competitive advantage; and, (3) to raise awareness among the American defense establishment that the Chinese Library Information System (LIS) serves as an enabler for “*juridical warfare*.”<sup>25</sup> This paper is based on a thorough survey

<sup>25</sup> *Juridical warfare* is defined by the author as the use/manipulation of law to obtain a military objective. See Harvey Rishikof, *Executive Summary—Juridical Warfare: The Neglected Legal Instrument*, JOINT FORCES Q., 1st QTR 2008, at 11, 11–12, [http://intelros.ru/pdf/jfq\\_48/7.pdf](http://intelros.ru/pdf/jfq_48/7.pdf) (discussing traditional paradigm of instruments of power, reviewing lawfare as a means to manipulate or control public perceptions, and describing Rishikof's preference for the term “juridical warfare,” which he defines as legal warfare that touches on any area of the administration of justice, over the narrower concept of “lawfare”). See generally Charles J. Dunlap, *Lawfare: A Decisive Element of 21st-Century Conflicts*, JOINT FORCES Q., 3rd QTR 2009, at 34, 35, <http://www.ndu.edu/press/lib/images/jfq-54/12.pdf> (defining “lawfare” as the

of secondary materials. It is presented with the belief that it will assist legal professionals, businessmen, researchers, and analysts in the protection of trade secrets and development of patent strategies.

## II. THE BATTLE SPACE

Make no mistake, the United States is at war with China.<sup>26</sup> Although unnoticed and generally unseen, libraries are on the frontlines.<sup>27</sup> In early January 2011, the Associated Press quoted U.S. Defense Secretary Gates regarding this competitor State. Although Gates did not specifically say that the United States is engaged in open conflict, he did say that “they clearly have potential to put some of our capabilities at risk. We have to pay attention to them, we have to respond appropriately with our own programs.”<sup>28</sup> China’s development of its stealth jet appears to have outpaced U.S. intelligence

---

“strategy of using-or misusing-law as a substitute for traditional military means to achieve an operational objective”).

<sup>26</sup> See Sy Harding, *Why China is Winning the Economic War—Nation Making Inroads, Even in Areas Where U.S. is Dominant*, FORBES, Aug. 16, 2010, [http://www.msnbc.msn.com/id/38726105/ns/business-forbes\\_com/t/why-china-winning\\_economic\\_war/#.Tr2GS2CXtaV](http://www.msnbc.msn.com/id/38726105/ns/business-forbes_com/t/why-china-winning_economic_war/#.Tr2GS2CXtaV) (describing China as the true economic powerhouse and discussing China’s impressive global inroads and the difficulty of U.S. companies in transporting dominance into the Chinese market and separately noting China’s graduating of 500,000 engineering students compared to 150,000 in the U.S., much of which is due to China’s massive population about which America can do nothing); Peter Navarro & Greg Autry, *China’s War on the U.S. Economy*, SFGATE.COM, Jan. 15, 2010, [http://articles.sfgate.com/2010-01-15/opinion/17828392\\_1\\_security-](http://articles.sfgate.com/2010-01-15/opinion/17828392_1_security-review) review commission china’s internet currency manipulation (noting that China’s targeting objective in its war on the U.S. economy was any intellectual property that would give Chinese enterprises the competitive edge – from trade secrets and new technologies to software such as Google’s proprietary source code). Compare Michael Sirak & Marc Schanz, *Space Arms Race? No*, AIR FORCE MAG., Aug. 2007, at 11–12 (discussing the intent to reduce tensions with China on space issues through dialogue), and Robert S. Dudley, *The China Gap—Editorial*, AIR FORCE MAG., Aug. 2010, at 2 (noting China’s military technology advancements and highlighting that only one side is racing), with Jan M. Van Tol, et. al., *Chart Page—The Long Reach of China’s Weapons*, AIR FORCE MAG., Aug. 2010, at 16 (portraying the ranges of China’s missiles and aircraft and highlighting China’s “anti-access” barrier strategy). See generally Richard Halloran, *China Stands Up*, AIR FORCE MAG., Aug. 2007, at 24–30 (discussing China’s existence as a military danger); Richard Halloran *China Turns up the Heat*, AIR FORCE MAG., Apr. 2010, at 34–37 (discussing the Chinese military’s hard push into “cyber warfare, anti-access weapons, and other means to blunt U.S. advantages”); John A. Tirpak, *Washington Watch: China Ramps up Offensive . . . to Expand its Military Power*, AIR FORCE MAG., Jan. 2010, at 7–8 (discussing China’s increased military capabilities).

<sup>27</sup> See generally Libicki, *supra* note 16.

<sup>28</sup> Gates Says China Moving Fast on New Weapons, FOXNEWS.COM, Jan. 9, 2011, <http://www.foxnews.com/world/2011/01/09/gates-says-china-moving-fast-new-weapons/print>.

estimates.<sup>29</sup> Its development of strategic ballistic missiles capable of hitting an aircraft carrier 2,000 miles away or intercepting space targets have also proven worrisome.<sup>30</sup> China's defense minister Liang Guanglie has responded by saying that "the efforts that we place on research and development of weapons systems are by no means targeted at any third country or any other countries in the world, and it will by no means threaten any other country in the world."<sup>31</sup> Both statesmen avoided mentioning China's advocacy of juridical warfare<sup>32</sup> and the critical role libraries play in the development of these programs.<sup>33</sup>

Clauswitz has described the "Art of War" to include all activities that exist for the sake of war.<sup>34</sup> Modern Chinese military theorists have declared that warfare "transcends all boundaries and limits, in short: unrestricted warfare."<sup>35</sup> Amidst this battle-space, libraries and librarians have emerged as precious national resources, with both being useful and vulnerable to warfare in various strata. These strata include: resource warfare (attacking information resources/holdings either directly or indirectly), regulatory warfare (leveraging information resources to develop patent or regulatory barriers to development), trade warfare (using information resources for competitive trade advantage), cyber warfare (applying library resources as an enabler for cyber technology's legal/illegal acquisition of digital resources), and technological development warfare (relying on information resources to make surprise advancements in high technology areas). Although librarians may not be considered spies,<sup>36</sup>

---

<sup>29</sup> *Id.*

<sup>30</sup> Anne Gearan, *US, China Defense Chiefs Mend Frayed Military Ties*, WASH. TIMES, Jan. 10, 2011, <http://www.washingtontimes.com/news/2011/jan/10/us-china-defense-chiefs-mend-frayed-military-ties>; see also SHIRLEY KAN, CONG. RESEARCH SERV., 110TH CONG., REPORT ON CHINA'S ANTI-SATELLITE WEAPON TEST, RS22652 (Apr. 23, 2007), available at <http://www.fas.org/sgp/crs/row/RS22652.pdf> (providing a governmental perspective on China's anti-satellite test); As *China's Army Flexes Its Muscles, a Missile is Intercepted in Space*, THE ECONOMIST, Jan. 14, 2010, available at <http://www.economist.com/node/15271130/print> (discussing China's openly bold testing of anti-satellite capabilities).

<sup>31</sup> Ben Blanchard & Chris Buckley, *China's Defense Minister Says Military Hardware Drive No Threat*, REUTERS, Jan. 10, 2011, <http://www.reuters.com/article/2011/01/10/us-china-usa-defence-idUSTRE7090Z620110110>.

<sup>32</sup> See generally Rishikof, *supra* note 2 (discussing traditional paradigm of instruments of power, reviewing lawfare as a means to manipulate or control public perceptions, and noting a preference for the term juridical warfare over lawfare, defining the concept more broadly as warfare that touches on any area of the administration of justice).

<sup>33</sup> See generally Jinxia Huang, *supra* note 18.

<sup>34</sup> CARL VON CLAUSWITZ, ON WAR 176 (Michael Howard & Peter Paret eds. & trans., 1976).

<sup>35</sup> QIAO LIANG & WANG XIANGSUI, *supra* note 24, at 12.

<sup>36</sup> See generally David Cho & Ariana Eunjung Cha, *Chinese Spying is a Threat Panel Says*, WASH. POST, Nov. 16, 2007, at A09 (discussing the bipartisan U.S.-China Economic and Security Review Commission and its conclusions that Chinese spying in the United States was the



libraries and librarians are no longer just sources of propaganda during the time of warfare.<sup>37</sup> They are now involved, both wittingly and unwittingly, in the full scope of knowledge management (KM)<sup>38</sup> necessary to science and technology collection and development.<sup>39</sup>

### III. JURIDICAL WARFARE STRATEGY

One would be remiss not to think that China includes its National Science Library's (NSL) (LIS) in its strategic warfare plan. Indeed, senior officials from the NSL have made open international presentations indicating that their libraries play a critical strategic role in the information and intelligence arena.<sup>40</sup> Doctrinally, China's LIS development falls in line with its "Three Warfares" strategy<sup>41</sup> (*Zhong Zhanfa*) approved by the Communist Central

---

biggest threat to keeping American technology secrets and noting that advances by the Chinese military are catching U.S. intelligence officials by surprise).

<sup>37</sup> See generally Ashley M. Smith, *American Libraries in Wartime: The Role of Propaganda* (Apr. 2007) (Master's Paper, University of North Carolina at Chapel Hill), available at <http://etd.ils.unc.edu/dspace/bitstream/1901/363/1/ashleysmith.pdf> (examining the spread of propaganda through public libraries during several periods of military conflict in American history).

<sup>38</sup> *Knowledge Management* is arguably broader in scope than traditional Competitive Intelligence practices, which are generally used to describe business-to-business collection and analysis. See France Bouthillier & Tao Jin, *CI Professionals and Their Interactions with CI Technology: A Research Agenda*, 3 J. OF COMPETITIVE INTELLIGENCE & MGMT. 41, 43 (2005) (discussing the rapid development of Competitive Intelligence software packages and the scope of Knowledge Management).

<sup>39</sup> As of 2010, China has had librarian representation at Strategic Competitive Intelligence Professionals (SCIP) annual meetings and other Competitive Intelligence conferences. See, e.g., *Schedule*, SECOND INT'L FORUM ON TECHNOLOGICAL INNOVATION & COMPETITIVE TECHNICAL INTELLIGENCE, <http://www.bjstinfo.com.cn/iticti08/content/list79.htm> (last visited Nov. 11, 2011) (providing an overview of numerous Chinese attendees from library and information management fields at a forum that was designed to demonstrate specific applications and best practices of competitive technical intelligence in kinds of industries and enterprises). From attendance, clearly, Chinese libraries are seeking to implement the same tools.

<sup>40</sup> See, e.g., Jinxia Huang, *supra* note 18; Liu Xiwen, *supra* note 23 (both presentations discussing the intelligence role of Chinese science and technology libraries).

<sup>41</sup> See generally Timothy Walton, *Treble Spyglass*, *Treble Spear: China's "Three Warfares,"* 4 DEFENSE CONCEPTS 49–60 (2009) (discussing Chinese Communist Party (CPC) Central Committee and the Central Military Commission (CMC) 2003 approved concept of "Three Warfares" and noting that the concept is developed for both military and non-military operations); *id.* at 60–61 (discussing *Legal Warfare*). Although Chinese doctrine of legal warfare appears to be directed primarily at political ends, the strategy cannot be separated from its science and technology developments when sovereignty of its actions is at play. Information warfare has assumed a central role in Chinese military writings in the psychological, media, and legal realms. *Id.*

Party.<sup>42</sup> Chinese libraries are viewed as a scientific discipline.<sup>43</sup> Its "Science of Military Strategy" describes an active defense as taking the initiative to annihilate the enemy.<sup>44</sup> Comparatively, these libraries are designed to gain strategic advantage in the juridical warfare arena after a competitor has promulgated an innovation. By design, they will be used to seize, database, and exploit breaking information resources through overt, legal, precise, and low profile Offensive Research Techniques (ORT).<sup>45</sup> Their purpose is to rely on both domestic and international laws to indigenously obtain, maintain, and defend patents and new technology developments.<sup>46,47</sup> The key means of

---

<sup>42</sup> See OFFICE OF THE SEC'Y OF DEF., 111TH CONG., ANNUAL REPORT ON THE MILITARY POWER OF THE PEOPLE'S REPUBLIC OF CHINA 2009 [hereinafter MILITARY POWER 2009], [http://www.defense.gov/pubs/pdfs/China\\_Military\\_Power\\_Report\\_2009.pdf](http://www.defense.gov/pubs/pdfs/China_Military_Power_Report_2009.pdf) (last visited Jan. 7, 2012) (discussing in the *Executive Summary* the impact of Chinese capabilities that allow this Competitor State to project power to ensure access to resources or enforce claims to disputed territories); see also OFFICE OF THE SEC'Y OF DEF., 111TH CONG., ANNUAL REPORT ON THE MILITARY AND SECURITY DEVELOPMENTS INVOLVING CHINA 2010, [http://www.defense.gov/pubs/pdfs/2010\\_CMPR\\_Final.pdf](http://www.defense.gov/pubs/pdfs/2010_CMPR_Final.pdf) (last visited Jan. 7, 2012) (providing an update on China's power projection).

<sup>43</sup> See GONG YITAI & G.E. GORMAN, LIBRARIES AND INFORMATION SERVICES IN CHINA 42 (2000) ("In the specialized research environment of CAS, library and information services are regarded as an integral part of scientific research and development."); Xiaoqing Ding et al., *Document Digitization Technology and Its Application for Digital Library in China*, in PROCEEDINGS OF THE FIRST INTERNATIONAL WORKSHOP ON DOCUMENT IMAGE ANALYSIS FOR LIBRARIES (2004) (providing an example of the type of focused literature on the scientific and technical engineering of library structures for efficiency and performance).

<sup>44</sup> See MILITARY POWER 2009, *supra* note 43, at 10–11 (discussing China's "Active Defense").

<sup>45</sup> *Compare Intellectual Property Theft in China and Russia: Hearing Before the Subcomm. on Courts, the Internet, and Intell. Prop.*, 109th Cong. (2005), <http://www.access.gpo.gov/congress/house/pdf/109hrg/21217.pdf> (focusing primarily on the illicit nature of China's counterfeiting and piracy of intellectual property and failing to discuss the legal tools in place for fostering China's indigenous innovation), with *China's Intellectual Property Rights and Indigenous Innovation Policy: Hearing Before the U.S.-China Econ. & Sec. Rev. Comm.*, 112th Cong. (2011), [http://www.uscc.gov/hearings/2011hearings/transcripts/11\\_05\\_04\\_trans/11\\_05\\_04\\_final\\_transcript.pdf](http://www.uscc.gov/hearings/2011hearings/transcripts/11_05_04_trans/11_05_04_final_transcript.pdf) (most hearings do not address the underlying causes/methods of intellectual property theft and therefore discuss solutions in only broad terms).

<sup>46</sup> Chinese lawyers are well prepared to tackle juridical warfare issues. See, e.g., Professor Claude Bruderlein, Comments at the Texas International Law Journal Symposium: The Air and Missile Warfare Manual: A Critical Analysis (Feb. 10–11, 2011) (noting that People's Republic of China lawyers, specifically, People's Liberation Army lawyers, were actively engaged in the dialogue over The Air and Missile Warfare Manual and also noting that an early circulation of a Chinese language draft unexpectedly presented itself in meetings and Chinese PLA lawyers showed themselves well versed in topics at hand) (on file with author).

<sup>47</sup> See *President Hu Stresses Significance of Sci-Tech Innovation in Global Competition*, ENGLISH.XINHUANET.COM, Mar. 15, 2011, [http://news.xinhuanet.com/english2010/china/2011-03/15/c\\_13780034.htm](http://news.xinhuanet.com/english2010/china/2011-03/15/c_13780034.htm) (providing an

their effectiveness are advanced software tools and collaboration.<sup>48</sup>

Today a Competitor State can leverage Library Information Systems for both political purposes and technology development.<sup>49</sup> This includes harvesting resources for the implementation of strategic national programs, (be they civil or military), leadership analysis for state decision making, and, profiling for targeting purposes.<sup>50</sup> For purposes of this paper, "targeting" in the science and technology context is the identification and aggressive pursuit of pre-competitive data at its most nascent stages. China's NSL appears to fill all three roles. Its identified intelligence purpose is to implement national development programs from cradle to grave.<sup>51</sup> It is also designed to support state decision making, and more tactically oriented exploitation of information for Chinese project implementation.<sup>52</sup> For this Competitor State, there's virtually no grammatical or legal distinction between *Qingbao*—intelligence; and, *Ziliao*—data, information, material.<sup>53</sup>

---

overview of Chinese leadership perspective on what is driving China's indigenous innovation policy and quoting Chinese President Hu Jintao that "enhancing the country's sci-tech innovation capacity is the key to accomplishing the tasks of the 12th Five-Year Program and taking the initiative in global competition"); see also *China's Indigenous Innovation Policy: Hearings Before the U.S. China Econ. & Sec. Review Comm'n*, 112th Cong. (2011) (testimony of Alan Wm. Wolff, Dewey & LeBoeuf LLP), [http://www.uscc.gov/hearings/2011hearings/written\\_testimonies/11\\_05\\_04\\_wrt/11\\_05\\_04\\_wolff\\_testimony.pdf](http://www.uscc.gov/hearings/2011hearings/written_testimonies/11_05_04_wrt/11_05_04_wolff_testimony.pdf) (outlining the development of China's indigenous innovation policies by citing various Chinese officials and specifically highlighting regional policy tools by quoting the Shanghai Municipal Government Announcement of Sep. 14, 2004: "[We shall] actively promote the formulation and implementation of technical standards with self owned intellectual property rights and translate that technological advantage into a marketplace advantage to maximize the benefits of intellectual property rights. [We shall] actively take part in the formulation of international standards, and drive the transferring of domestic technological standards to international standards . . .").

<sup>48</sup> See Jinxia Huang, *supra* note 18; Liu Xiwen, *supra* note 23 (both discussing the use of networks and collaborations between China's national science and technology libraries and universities).

<sup>49</sup> See Jinxia Huang, *supra* note 18; Liu Xiwen, *supra* note 23 (both discussing the political decision making role played by China's National Science Library).

<sup>50</sup> See Jinxia Huang, *supra* note 18; Liu Xiwen, *supra* note 23 (both discussing the use of networks and collaborations between China's national science and technology libraries and universities).

<sup>51</sup> See Liu Xiwen, *supra* note 23, at Slide 7 (discussing the process of China's libraries data collection, project identification, project decision making, strategy planning, and project implementation of science and technology programs).

<sup>52</sup> *Id.*

<sup>53</sup> Huo Zhongwen & Wang Zongxiao, *Sources and Techniques of Obtaining National Defense Science and Technology Intelligence*, FED'N OF AM. SCIENTISTS, <http://www.fas.org/irp/world/china/docs/sources.html#comment> (last visited Jan. 11, 2011) (providing an explanation of Chinese interpretation of intelligence and information in the

Although China's NSL appears to be a benign establishment, secondary research shows it emerging as a critical enabler for technological advancement.<sup>54</sup> It is, however, a low profile<sup>55</sup> collector, (the activities of its staff and customers are low visibility).<sup>56</sup> China's NSL does not appear to attract much outside attention—there were only forty-six visitors to its website in early January 2011.<sup>57</sup> Still, it appears to be gaining influence and prestige both internally and on the international scene.<sup>58</sup> Librarians of the People's Republic are relishing in their new roles as information warriors.<sup>59</sup> China understands that whoever has the better library has both the wartime and peacetime advantage.<sup>60</sup> The NSL's mission and architecture are purposed to deliver

---

Editor's Comment).

<sup>54</sup> See Jinxia Huang, *supra* note 18; Liu Xiwen, *supra* note 23 (both discussing the use of networks and collaborations between China's national science and technology libraries and universities).

<sup>55</sup> *Low-Profile* is defined as "a deliberately inconspicuous, almost unnoticeable form." THE RANDOM HOUSE COLLEGE DICTIONARY 795 (Rev. ed.1984); *accord* WEBSTER'S NEW WORLD DICTIONARY 802 (3d college ed. 1991) (providing an alternative definition of "an unobtrusive, barely noticeable presence, concealed, inconspicuous activity"). The author is relying on the plain English meaning of Low Profile. This is a term frequently utilized in law enforcement and intelligence circles to mean not drawing attention to plans, activities, or discussions. Activities of librarians are by their very nature low-profile, they would not otherwise be suspected of clandestine government associations.

<sup>56</sup> See *generally Low-Visibility Operations Definition*, DOD DICTIONARY OF MILITARY TERMS, [http://www.dtic.mil/doctrine/dod\\_dictionary/?zoom\\_query=low+visibility&zoom\\_sort=0&zoom\\_per\\_page=10&zoom\\_and=1](http://www.dtic.mil/doctrine/dod_dictionary/?zoom_query=low+visibility&zoom_sort=0&zoom_per_page=10&zoom_and=1) (last visited Jan. 11, 2012). The author acknowledges that foreign governments may use librarians and library information systems to conduct low visibility operations – otherwise sensitive collection operations wherein the political-military restrictions inherent in covert and clandestine operations are either not necessary or not feasible; actions are taken as required to limit exposure of those involved and/or their activities. Execution of these operations is undertaken with the knowledge that the action and/or sponsorship of the operation may preclude plausible denial by the initiating power. Traditionally, libraries are not viewed as an implement of modern warfare. See *generally* Michael Howard, *Afterword to TOOLS OF WAR* 238–246 (John A. Lynn ed., 1990) (discussing the traditional "concepts and technology" of war).

<sup>57</sup> See NAT'L SCI. LIBR., CHINESE ACAD. OF SCI., <http://english.las.cas.cn> (last visited Jan. 11, 2012), for access to the NSL website.

<sup>58</sup> See Jinxia Huang, *supra* at note 18; Liu Xiwen, *supra* note 23 (demonstrating the global reach of Chinese library officials).

<sup>59</sup> See Elizabeth Graham & Roberta Sparks, *Libraries as a Catalyst for Economic Growth and Community Development: A Mayor's Summit on Public Libraries*, 86 TEX. LIB. J., 30, 30 (2010) (noting China's participation in the event).

<sup>60</sup> See SUN TZU, *supra* note 1, at 15 ("To fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting. In the practical art of war, the best thing of all is to take the enemy's country whole and intact; to shatter and destroy it is not so good. So, too, it is better to capture an army entire than to destroy it, to capture a regiment, a detachment or a company entire than destroy them.").

information resources to the customer with rapidity. It is designed to produce surprise “out-of-the blue” developments in high-end technology fields.<sup>61</sup> Both rapidity and surprise are components of Sun Tzu’s philosophy in *The Art of War*.<sup>62</sup> What we might call good espionage, the Chinese simply refer to as excellent information management.<sup>63</sup>

#### IV. The Emerging Library Model—S&T Targeting Centers

By popular definition, a library is a collection of sources, resources, and services.<sup>64</sup> Historically, the American concept of a library has been an institution with rows upon stacks upon books. With the emergence of the World Wide Web, images of researchers in dusty parlors have given way to views of academics downloading digital information resources from global access points at local cafes. China itself has a long library tradition that dates back to its ruling dynasties of Imperial China, from 221 to 206 B.C.,<sup>65 66</sup>

---

<sup>61</sup> Cf. DEITCHMAN, *supra* note 5, at 201 (discussing how new technology developments appear “out-of-the-blue,” but in actuality have long backgrounds of experimental and theoretical accumulation of knowledge).

<sup>62</sup> See SUN TZU, *supra* note 1, at 26 (“He who is skilled in attack flashes forth from the topmost heights of heaven, making it impossible for the enemy to guard against him. This being so, the places that he shall attack are precisely those that the enemy cannot defend.”); cf. Cho & Cha, *supra* note 36 (discussing technology advancements catching U.S. intelligence personnel by surprise).

<sup>63</sup> See generally Huo Zhongwen & Wang Zongxiao, *supra* note 53 (discussing Chinese information management strategy).

<sup>64</sup> See generally THE NEW ENCYCLOPAEDIA BRITANNICA 947–63 (15th ed. 2010) (discussing modern definition of library and noting the rapid development in computers, telecommunications, and other technologies trending toward digital and virtual libraries).

<sup>65</sup> See GONG YITAI & G.E. GORMAN, *supra* note 43, at 1–84, for background and history on Chinese libraries. A system of writing and collection of works began to appear at the earliest stages of Chinese culture under the Shang Dynasty 1700–1600 B.C. *Id.* at 3. China’s earliest collections were organized as official archives by the government and private institutions or wealthy families. *Id.* By the Qin Dynasty 221–206 B.C. the government had introduced a system of scripts for the collection and preservation of records by the central government. *Id.* at 5. The Han Dynasty followed in 206 B.C.–220 A.D. and was notable for “importing ideas and practices from foreign civilizations” and early collections were accompanied by the government’s establishment of the Office of Secret Records responsible for managing records, analyzing their content, and undertaking comparative studies. *Id.* at 6. By contrast, China’s earliest written records appeared on wood, stone, pottery, leather, bone, tortoiseshell, and metals, but from the beginning written records were held as highly important to Chinese civilization. *Id.* at 3.

<sup>66</sup> See SHARON CHIEN LIN, LIBRARIES AND LIBRARIANSHIP IN CHINA 119–31, 180–81, 185–211(1998), for background and history on Chinese Special Libraries. As of 1998, research China’s research activities were concentrated in the Chinese Academy of Sciences, consisting of over 143 research institutes and laboratories spread through China, and a staff of over 82,326. *Id.* at 118. Chinese libraries have been recognized as catalysts for the advancement of science and technology, and are found in private businesses, industrial organizations and professional

While China's original written holdings were written on bones and tortoise shells,<sup>67</sup> now its primary focus is on digital library (DL) resources.<sup>68</sup> The NSL's DL resources and applications are designed to be collaborative in nature.<sup>69</sup> Collaborative, however, is a relative term, as the NSL is designed to connect holdings within China through library consortia,<sup>70</sup> and not necessarily share them with foreign partners or researchers.<sup>71</sup>

Today, China's National Science Library is pioneering new concepts of library research through computational methodologies,<sup>72</sup> scientometrics,<sup>73</sup> bibliometrics,<sup>74</sup> citation and co-author analysis,<sup>75</sup> and visualization research.<sup>76</sup>

---

societies. *Id.* at 122. These Document Information Centers (DIC) and Science and Technology Information Centers (STI), are supported and maintained by government agencies and institutions. *Id.* Among its missions, the CAS Library Information System is to "collect, process, exploit, and provide Chinese and foreign sci-tech literature in accordance with the research orientation and responsibilities of CAS." *Id.* at 126. It is also "to carry out analysis and study of foreign and domestic sci-tech information and provide information services catering to the needs of CAS (formulating developmental strategies, policies, and plans, and organizing major research projects)." *Id.*

<sup>67</sup> GONG YITAI & G.E. GORMAN, *supra* note 43, at 3.

<sup>68</sup> See Jinxia Huang, *supra* note 18; Liu Xiwen, *supra* note 23 (both presentations discussing the use of networks and collaborations between China's national science and technology libraries and universities).

<sup>69</sup> *Id.*

<sup>70</sup> See generally Elaine Xiaofen Dong & Tim Jiping Zou, *Library Consortia in China*, 19 LIBR. & INFO. SCI. RES. ELECTRONIC J. 1, 1–10 (2009), [http://libres.curtin.edu.au/libres19n1/Dong\\_Essay\\_Op.pdf](http://libres.curtin.edu.au/libres19n1/Dong_Essay_Op.pdf) (discussing library consortia in China and the fact that most; stating also that Chinese libraries are partially or fully supported by the government and that national library consortia began to emerge in the late 1980s. Some larger consortia include reciprocal programs with foreign library systems).

<sup>71</sup> See Jinxia Huang, *supra* note 18; Liu Xiwen, *supra* note 23 (both presentations discussing the intelligence role of Chinese science and technology libraries).

<sup>72</sup> See Interview with Susan Ardis, Head, Eng'g & Sci. Libraries Div., Univ. of Tex. at Austin (Feb. 10, 2011) (noting that Chinese libraries such as Tsinghua University may have some limited interlibrary loan services, however, technical, linguistic, and cultural barriers still preclude full transparency as to holdings).

<sup>73</sup> See generally VIRGIL DIODATO, *DICTIONARY OF BIBLIOMETRICS* viii–x (1994) (discussing Bibliometrics and Scientometrics). Bibliometrics and Scientometrics utilize mathematical and statistical modeling to determine what areas of research are being pursued in any given field. *Id.* Scientometrics focuses on citation analysis in the field of science and technology while Bibliometrics is more general in nature. *Id.*

<sup>74</sup> See generally NICOLA DE BELLIS, *BIBLIOMETRICS AND CITATION ANALYSIS* xi–xiii (2009) (noting that Bibliometrics is the quantitative analysis and measurement of literature while Scientometrics focuses on the measurement of change in science and technology innovation as presented in science literature).

<sup>75</sup> Rulmin Ma et al., *An Author Co-Citation Analysis of Information Science in China with Chinese Google Scholar Search Engine, 2004–2006*, 81 SCIENTOMETRICS 33, 33–46, available at <http://www.springerlink.com/content/f2wg100412467351/> (last visited Jan. 11, 2012)

The library network is designed to *harvest*<sup>77</sup> breaking information at the earliest stages of open research.<sup>78</sup> Collection centers are instituted to generate synergy and collaboration among State influenced academic and commercial entities.<sup>79</sup> The State-directed acquisition of this research creates a competitive advantage for Chinese researchers.<sup>80</sup> LIS services cover the entire spectrum of an intelligence collection cycle—targeting, direction, collection, processing, analysis, and exploitation.<sup>81</sup>

China's use of a "novelty search" provides a perfect example of its use of intelligence tools as a means to advance science and technology research.<sup>82</sup> The Scientific and Technological Project Search Service offered by the Chinese Academy of Science Library Information System provides "comprehensive information searches to meet the background needs of a

---

(providing an abstract on author co-citation analysis).

<sup>76</sup> Sophie L. Rovner, *Measured by Patent Applications or Journal Articles, Growth in Chinese Scientific Output is Stupendous*, 88 CHINA ASCENDANT 35–37 available at

<http://pubs.acs.org/cen/science/88/8802sci1.html?featured=1> (last visited Jan. 11, 2012)

(providing an example of visualization and horizon mapping in Chinese patents and stating that the tremendous growth in Chinese chemical patenting and publishing is being driven by the combination of economic development and awareness of the strategic importance of intellectual property protection, and also quoting Sunny Wang, 2009 president of the Tri-State chapter of the Chinese American Chemical Society).

<sup>77</sup> "Harvest" s defined by the author as not only collecting information, but being able to efficiently cultivate resources for predatory exploitation against a competitor.

<sup>78</sup> Jinxia Huang, *supra* note 18; See also Liu Xiwen, *supra* note 23 (both presentations discussing China's use of alert services).

<sup>79</sup> See generally PRISCILLA C. YU, CHINESE ACADEMIC AND RESEARCH LIBRARIES:

ACQUISITIONS, COLLECTIONS, AND ORGANIZATIONS, 149 (1996) (highlighting the collaborative nature of Chinese libraries and noting that the "largest and most complex database for the Chinese Academy of Sciences, Chengdu, ist he national patent file" and ist technical holdings contain 50% foreign journals). Cf. Conference Report, Int'l Fed'n of Library Ass'n & Inst., Wu Jianzhong, Transition to an e-and-globalised age: Shanghai Library's Practice of Change (Aug. 13–18, 2011), [http://conference.ifla.org/past/ifla77/123\\_jianzhong-en.pdf](http://conference.ifla.org/past/ifla77/123_jianzhong-en.pdf) ("[M]odern librar[ies] should not only actively participate in the knowledge dissemination and innovation for the general public, but also actively participate in the government decision making and policy consultation, the research and innovation of research groups, as well as the industrial development for corporations and freelandes.").

<sup>80</sup> See Hu Junping, *Special Libraries in China: Present and Future*, WHITE CLOUDS, LLC (Feb.17, 2011), <http://www.white-clouds.com/iclc/cliej/cl1huj.htm> (discussing China's 3700 libraries and national direction of its Special Library system).

<sup>81</sup> Jinxia Huang, *supra* note 18; Liu Xiwen, *supra* note 23 (both presentations discussing the intelligence role of Chinese science and technology libraries).

<sup>82</sup> See Jing Liu & Yiliang Song, *The Impact of Technology of Chinese Library Collections and Services*, in THE IMPACT OF TECHNOLOGOGY ON ASIAN, AFRICAN, AND MIDDLE EASTERN LIBRARY COLLECTIONS, LIBRARIES AND LIBRARIANSHIP 76 (R.N. Sharma ed., 2006) (providing a detailed look at new information technologies in China's library operations).

particular project.”<sup>83</sup> By design, this service scours electronic science and technology holdings, print materials, and research banks to determine the “state of the art of a particular research field to determine whether a particular project has been done, what has been done, how it has been done, and how many research articles or other materials are related to the subject.”<sup>83</sup> By design, this service scours electronic science and technology holdings, print materials, and research banks to determine the “state of the art of a particular research field to determine whether a particular project has been done, what has been done, how it has been done, and how many research articles or other materials are related to the subject.”<sup>84</sup> As of 2006, at least forty-three academic libraries had been given the authority to implement novelty searches.<sup>85</sup> “Scientists or researchers who apply for research funding, grants, patent registration, or academic awards are requested to submit their application with a Scientific and Technological Project Search Service Report.”<sup>86</sup> The use of these services provides Chinese scientists and researchers with state-supported situational awareness necessary to remain competitive in high-tech fields.

NSL implements its collaborative approach with leading universities and institutions throughout China to harness resources for exponential gains across multiple disciplines.<sup>87, 88</sup> As a “Targeting Center”<sup>89</sup> for emerging and breaking technology, the NSL has essentially developed a science and technology wellspring from which Chinese innovators can obtain leads for creative implementation of State goals. Once an emerging technology or innovation is

---

<sup>83</sup> *Id.* at 86.

<sup>84</sup> *Id.*

<sup>85</sup> *Id.*

<sup>86</sup> *Id.*

<sup>87</sup> Ben Gu, *Chinese Resource Development in the National Library of China* (Feb. 26, 2009), [http://www.varastokirjasto.fi/beijing/GU\\_ben.pdf](http://www.varastokirjasto.fi/beijing/GU_ben.pdf); see also *Development of Science and Technology in China*, EMBASSY OF THE PEOPLE'S REPUBLIC OF CHINA IN THE HELLENIC REPUBLIC (Aug. 3, 2004), <http://gr.chinaembassy.org/eng/kxjs/zgkj/t146165.htm> (noting that Chinese higher education institutions are an active contingent in China's scientific and technological front and providing only statistics from 1998 that Chinese universities were associated with close to 1,500 research and development institutions).

<sup>88</sup> While many scholars focus on the positive aspects of Collaborative Research, few have focused on the dangers of pre-patent technology theft, which may arise from collaborative international research. See, e.g., Robert M. Hayes, *Comparative Research*, in *AREAS OF COOPERATION IN LIBRARY DEVELOPMENT IN ASIA AND PACIFIC REGIONS* 16, 16–18 (Sally C. Tseng et al. eds., 1985) (discussing the value of collaborative international research but failing to mention pre-patent technology theft).

<sup>89</sup> “Targeting Center” is defined by the author as any public or private institution designed to increase the precision of collection of pre-competitive science and technology data for exploitation by either civil or military researchers.



identified, the LIS architecture and NSL research tools allow the full weight of a research team to be quickly assembled and brought to bear upon breaking information. That research team then receives full support from this Competitor State's collection apparatus including resources and advisement of subject-matter librarians. The ultimate goal is indigenous innovation.<sup>90</sup>

## V. THE TARGET—NEWNESS AND INNOVATION

Chinese libraries are integrated directly into its Chinese patent strategy. Separate studies have shown that China is building a "Great Wall of Patents" to protect its development of high-technology.<sup>91</sup> The process is simple. The Chinese are filing for patents in China on the patents they are copying.<sup>92</sup> China's strategy has been to review digital patent applications posted on foreign websites then file and obtain patents on early stage technologies inside China to propel key technology development.<sup>93</sup> As Chinese companies have strong ties to the national government, their use of American patent information can easily blur the lines between civil and military applications.<sup>94</sup> Additionally, China's patent strategy costs American businesses an estimated \$50 billion per year in lost revenues as companies defend their innovations.<sup>95</sup>

China's NSL provides an additional advantage for Chinese companies. The LIS collection of breaking science and technology information at its earliest stages combined with the availability of online patent filings and electronic research tools, allows Chinese developers to attack the legal precepts

<sup>90</sup> See *The Long Arm of the State—Government's Role in Industry—Innovation by All Means*, THE ECONOMIST, June 25, 2011, at 15 (discussing the Chinese government's support for development of indigenous Chinese innovation and impact of protectionist Chinese regulations on international competition).

<sup>91</sup> See Pat Choate, A Great Wall of Patents (Nov. 7, 2005) (unpublished working paper), [http://www.uscc.gov/researchpapers/2005/working\\_paper\\_nov\\_7\\_05.htm](http://www.uscc.gov/researchpapers/2005/working_paper_nov_7_05.htm) ("In China, as with all other nations, the patent office issues the patent to the first person to file an application. The burden of proving that the Chinese patent seeker stole the idea can take years and cost hundreds of thousands of dollars in legal fees. If the Chinese patent holder makes a few modifications in the application that burden is even more difficult.").

<sup>92</sup> *Id.* (providing an overview of Chinese patent strategy and its impact on U.S. manufacturing).

<sup>93</sup> *Id.* (noting that part of China's patent strategy has been to review patent filings posted on the web for competitive advantage).

<sup>94</sup> See QIAO LIANG & WANG XIANGSUI, *supra* note 24 ("War in the age of technological integration and globalization has eliminated the right of weapons to label war and, with regard to the new starting point, has realigned the relationship of weapons to war, while the appearance of weapons of new concepts, and particularly new concepts of weapons, has gradually blurred the face of war. Does a single 'hacker' attack count as a hostile act or not? Can using financial instruments to destroy a country's economy be seen as a battle?").

<sup>95</sup> Choate, *supra* note 91 (noting \$50 billion in losses to U.S. businesses per year due to Chinese patent pirating and counterfeiters).

necessary to later file and defend a patent. Since Chinese patent law recognizes those patent applications filed first, there is an incentive to provide early warning on innovative developments to Chinese entities.<sup>96</sup> Lawfare is thereby waged against newness, innovation, and usefulness.<sup>97</sup> Although critics claim China produces researchers less creative than Western innovators, this Competitor State is providing *Next-Gen* tools necessary to dominate new technological innovation.<sup>98</sup> The ability of libraries and library staff to collect and marshal resources with pinpoint accuracy increases the effects of China's Offensive Research Techniques (ORT)

#### VI. A HYPOTHETICAL

Take for the example the following hypothetical: A key U.S. academic working toward his PHD has come up with an innovative software code for aeronautical applications. Although his innovation is not yet patented, the innovation is extremely new, not obvious, clearly innovative, and useful. The U.S. academic is encouraged to present a Master's paper at a private but unclassified conference setting with limited public attendance.<sup>99</sup> The premise of the paper is purposed towards civil applications, but it could also provide significant military advancements in multiple fields. There is limited professional discussion regarding the conference among academics. The Master's paper is filed in the university's engineering library's holdings.

A Chinese student thereafter requests the paper from the student's engineering library. The request is ostensibly for personal research, but is realistically also to advance national science and technology objectives. The paper is obtained and filed in the National Science Library's digital holdings. Horizon Scanning tools map the information and an alert services early warning goes out to leading Chinese researchers in the field. National exploitation of

---

<sup>96</sup> *Id.* at 4 ("In China, as with all other nations other than the United States, the patent office issues the patent to the first person to file an application").

<sup>97</sup> See generally ARTHUR R. MILLER & MICHAEL H. DAVIS, *INTELLECTUAL PROPERTY: PATENTS, TRADEMARKS, AND COPYRIGHTS IN A NUTSHELL* 10 (4th ed. 2007) (providing an overview of newness, innovation, and usefulness in the context of patent law).

<sup>98</sup> THOMAS L. FRIEDMAN, *THE WORLD IS FLAT* 365 (2005) (interviewing Bill Gates about the American education advantage and Chinese desire to dominate the U.S. in innovation).

<sup>99</sup> It is well publicized that Chinese libraries actively pursue the collection of foreign conference proceedings, dissertations, and theses. See, e.g., Xue-Ming Bao, *The National Science and Technology Library: A Chinese Model of Collaboration*, *ISSUES IN SCI. & TECH. LIBRARIANSHIP* (Summer 2005), available at <http://www.istl.org/05-summer/article4.html> (displaying Table 1 NSTL Collection Statistics of Abstract Items dated Aug. 16, 2004 and identifying 2,078,805 foreign conference proceedings and 46,667 dissertations and thesis in its inventory). Given NSTL's mission to avoid duplication it is likely that each library networked to China's National Science Library collects dissertations, conferences proceedings, and theses in separate niche areas to avoid duplication.

the material occurs with the full weight of Chinese research teams being brought to bear on the science and technology development.

Co-author citation analysis occurs and the entire background of the student's research is assessed through various social networking tools. Chinese Offensive Research Techniques are employed in academic, commercial, and governmental settings. A large number of Chinese student researchers begin to write on the thesis or aspects of the innovation. Approaches are made to other leading experts in the field who have written on point. Their works are exploited through Co-Author Citation Analysis. The Principle of Mass takes over and Chinese research dominates the topic.<sup>100</sup> By the time the U.S. academic presents his PHD thesis, by Chinese standards, the innovation is no longer new, and, no longer non-obvious.

Chinese researchers rapidly file patents in China and advance technology applications with newness, innovation, and usefulness in both civilian and military arenas. Principles of juridical warfare manifest both RAPIDITY and SURPRISE. Further Chinese patents are developed around the innovation in a *Great Wall* strategy. Chinese researchers have therefore defeated U.S. academics on the high-ground of legal theory. Nothing in the Chinese tactical approach to the research is ostensibly illegal.

## VII. THE PROOF

Under patent law, a potential patentee must demonstrate that he/she has developed a (1) new, (2) useful, (3) non-obvious, (4) process/product.<sup>101</sup> So long as Chinese researchers can *legally* acquire documents on advanced theses and innovations and assemble them into its Library Information Systems, to perpetuate and excel further writing by Chinese scientists and researchers at whatever level, the argument can be made that a potential patentee's idea is not new, and not non-obvious. The national security implications are obvious. Unless a Western academic is astutely aware of the threat of State-supported open source collection, the National Science Library alert services, and its competitive research architecture, he or she can severely disadvantage himself or herself with the early release of proprietary technology research. Academics who are publicly releasing innovative theses or curricula are also vulnerable. Similarly, commercial patent libraries or data holdings, whether they are open to

---

<sup>100</sup> See DEP'T OF THE ARMY, U.S. ARMY FIELD MANUAL, NO. 3-0, FUNDAMENTALS OF FULL SPECTRUM OPERATIONS 4-2-4-31(2001), [http://www.dtic.mil/doctrine/jel/service\\_pubs/fm3\\_0a.pdf](http://www.dtic.mil/doctrine/jel/service_pubs/fm3_0a.pdf) (discussing the Principle of Mass as a concentration of the effects of combat power at the decisive place and time; comparatively, Chinese libraries allow collection efforts to be directed with precision to achieve similar dominance in the strategic environment).

<sup>101</sup> MILLER & DAVIS, *supra* note 97.

the public or private, are at risk by these same Competitor Collectors. As Chinese patentees get to *The Prize*<sup>102</sup> and file first, the small-caliber American innovator,<sup>103</sup> who generally has no such governmental or commercial backing, is at an extreme disadvantage.

#### VIII. COMPETITOR COLLECTORS

It is generally accepted as common fact that Chinese students are both formally and informally tasked to collect on requirements for Chinese State objectives.<sup>104</sup> Chinese consulates are said to maintain a list of persons with talent whom they encourage to collect against science and technology objectives.<sup>105</sup> The drive for student collection has been primarily toward overt acquisition of information rather than illicit activity.<sup>106</sup> Authors are often confused as to whether or not students are officially employed by the state. To this end, it is likely that Chinese students obtaining scholarships or visa support from Chinese Academy of Sciences (CAS) and/or Ministry of Science and Technology (MOST) do so with a *quid pro quo*. While on scholarship, they are collecting against the State's national science and technology objectives.<sup>107</sup>

The real threat then is not necessarily what Chinese students/researchers are collecting, but how it is applied in China's Library Information System. Until the mid 2000s, Western competitors did not have to worry so much about China's library system. In the 1990s it was just beginning to digitize its resources.<sup>108</sup> The State's ability to collect information far

<sup>102</sup> "*The Prize*" is defined by the author in this context as any patent that helps secure a science and technology advancement in a pivotal commercial or military field. Cf. DANIEL YERGIN, *THE PRIZE: THE EPIC QUEST FOR OIL, MONEY, AND POWER* (1991) (discussing the history of oil and the struggle for wealth and power surrounding the oil industry).

<sup>103</sup> See Dan Winters, *Atoms are the New Bits*, WIRED MAG., Feb. 2010, at 59 (discussing the garage-size inventor and advocating small caliber business with China but failing to discuss risks of patent infringement or costs of defending innovation).

<sup>104</sup> See Jeff Hayes, *Chinese Military, Hackers, and Cybernationalists*, <http://factsanddetails.com/china.php> (last updated Oct. 2011) (discussing generally accepted facts regarding United States, China, and Spies).

<sup>105</sup> *Id.*

<sup>106</sup> BILL GERTZ, *THE CHINA THREAT: HOW THE PEOPLE'S REPUBLIC TARGETS AMERICA* 131-34 (2000) (discussing unclassified handbook for Chinese spies and collection of unclassified information from U.S. laboratories and universities). See generally Huo Zhongwen & Wang Zongxiao, *supra* note 54 (providing background information from the Chinese perspective).

<sup>107</sup> The Chinese Library Information System is designed to capture open research for use against national priorities. See *Terrorism and Intelligence Operations: Before the Joint Econ. Comm.*, 105th Cong. (1998) (statement of Nicholas Eftimiades, Author, "Chinese Intelligence Operations") available at [http://www.fas.org/irp/congress/1998\\_hr/eftimiad.htm](http://www.fas.org/irp/congress/1998_hr/eftimiad.htm) (discussing cross-over between espionage and more open collection and the frequent use of Chinese travelers to collect information on national priorities).

<sup>108</sup> Liu Xiwen, *supra* note 23; see also Xihui Zhen, *Overview of Digital Library Development in*

outpaced its ability to manage its holdings. Today, however, secondary resources indicate that China is emerging as a powerhouse in library management.<sup>109</sup> Its emphasis on foreign acquisitions and digital holdings combined with its development of alert services capabilities should put Westerners on guard. "Now, any time a Western researcher puts something on the Internet [or files it in a Library] it can be directly leveraged by a foreign research team."<sup>110</sup>

The threat of Chinese students collecting against breaking U.S. science and technology developments has been well publicized.<sup>111</sup> Its integration with Chinese Library Information Systems and strategic incorporation into juridical warfare is, however, less understood. By 2008, there was a record number of Chinese students studying in the United States.<sup>112</sup> Even if not directed by the State, these students were taking on a spotting and assessing role, collecting new and emerging technological data on breaking theses and research work to be harvested by China's Library Information Systems.<sup>113</sup> China is on the offensive drive for science and technology

---

*China*, D-LIB. MAG. (May/June 2010), <http://www.dlib.org/dlib/may10zhen/05zhen.html> (reviewing the development of Chinese electronic libraries from the mid 1990s on).

<sup>109</sup> See Cong Cao, *Has China Become a Patent Powerhouse?*, UPI ASIA ONLINE (Feb. 10, 2009), <http://www.upiasia.com/Economics/2009/02/10/> (noting that China's increasing patent applications are the result of a change in China's strategy concerning scientific and technological development—from following others to taking the lead in building an indigenous innovation capability).

<sup>110</sup> See FRIEDMAN, *supra* note 98, at 369.

<sup>111</sup> See *Special Report: Espionage with Chinese Characteristics*, STRATFOR GLOBAL INTELLIGENCE (Mar. 24, 2010),

[http://web.stratfor.com/images/writers/INTEL\\_SERVICES\\_CHINA.pdf](http://web.stratfor.com/images/writers/INTEL_SERVICES_CHINA.pdf) (discussing Chinese nationals who are asked to acquire targeted technologies while traveling and the Chinese Student and Scholar Association, and also noting that China's intelligence services focus on business and technology intelligence rather than political intelligence); see also Bill Gertz, *Chinese Student Suspects in Espionage*, WASH. TIMES, <http://www.washingtontimes.com/news/2003/aug/4/20030804-112043-2685r/?page=all> (last visited Jan. 11, 2012) ("Two Chinese students studying in the United States supplied China's military with American defense technology . . ."); *New Chinese Spy Chief an Expert on Commercial Intelligence, Monitoring Group Says* (Aug. 31, 2007), [http://www.iht.com/articles/ap/2007/08/31/asia/AS-GEN\\_China\\_Spy\\_Chief.php](http://www.iht.com/articles/ap/2007/08/31/asia/AS-GEN_China_Spy_Chief.php) (discussing Geng Huichang and his former association with the China Institute of Contemporary International Relations and describing China's probable appeal to businesspeople and academics of Chinese origin to gain classified information on new technology, especially with possible military applications) (on file with author); SUN TZU, *supra* note 1, at 49 ("The ideal commander unites culture with a warlike temper; the profession of arms requires a combination of hardness and tenderness.").

<sup>112</sup> Jenifer Pak, *Overseas Education More Attainable for Chinese Students*, VOICE OF AM., Apr. 28, 2008, <http://www.voanews.com/english/news/a-13-2008-04-28-voa23.html>.

<sup>113</sup> See GERTZ, *supra* note 106, at 131–36 (arguing that the Chinese gather intelligence through

patents.<sup>114</sup>

### IX. Collection Strategy<sup>115</sup>

In 1999, the Director of CIA and FBI forwarded a joint letter to congress highlighting Beijing's top national security priority.<sup>116</sup> This priority was to collect science and technology information to advance China's economic development.<sup>117</sup> For over a decade, Chinese collection practices have been described with the following characteristics:

"China's collection of open source, sensitive, and restricted proprietary/trade secret U.S. technology and economic information, particularly advanced civilian, military, dual-use and bio-technology, remained a priority."

"China's official collectors of economic intelligence were noted to use collection methods that were low-key and nonthreatening."

"Chinese nationals working abroad lawfully gathered most S&T and economic intelligence through open sources, such as U.S. university libraries, research institutions, the Internet, and unclassified databases, providing the Chinese Government with highly valued, yet unclassified information."

"The Chinese intelligence services were noted to have a long history of using Chinese students studying abroad to collect information, either formally for those services or informally for their home-based research institutes or universities. "

"Many Chinese students in U.S. graduate schools were studying hard sciences and were able to collect a wide variety of information that is of value to China's efforts to ascend the technology ladder. "

"Because the Chinese considered themselves to be in a developmental "catch-up" situation, their collection program tended to have a comparatively broad scope. Chinese collectors targeted information and technology on anything of value to China, which led them to seek to collect open-source information as well as restricted/proprietary and classified information."<sup>118</sup>

---

the overt collection of technical information).

<sup>114</sup> Cong Cao, *supra* note 109 (discussing rising awareness in China of the importance of patents and intellectual property rights).

<sup>115</sup> Arguably the Chinese have positioned their researchers first on the technological battlefield. See SUN TZU, THE ART OF WAR 103 (Thomas Cleary trans., Shambhala Publ'ns 1st ed. 1988) (6th Cent. B.C.) ("Those who are first on the battlefield and await the opponents are at ease; those who are last on the battlefield and head into battle get worn out").

<sup>116</sup> Letter from George J. Tenet, Director, CIA & Louis J. Freeh, Director, FBI, to J. Dennis Hastert, Speaker of the House of Representatives (Dec. 12, 1999), *available at* [http://www.fas.org/irp/threat/fis/prc\\_1999.html](http://www.fas.org/irp/threat/fis/prc_1999.html).

<sup>117</sup> Interview with Susan Ardis, *supra* note 71.

<sup>118</sup> Letter from George J. Tenet, *supra* note 116.

The underlying thread in China's science and technology collection is primarily that (1) it is overt, (2) it is legal, (3) it is precise, and (4) it is focused collecting on the lowest possible level of breaking research possible—the undergraduate and postgraduate level. In this arena, theses go unpublicized, papers go unpublished, and competitors go unnoticed. From all accounts, the research looks perfectly benign.<sup>119</sup> That is unless the information is acquired, catalogued, and leveraged into a document retrieval center. Once there, the information is exploited for creative and specialized high-end and dual-use engineering leads.<sup>120</sup> Libraries provide that extra precision for ORT.

#### X. Motivation and Drive

Author Thomas L. Friedman in *The World is Flat* has adequately addressed the drive behind Chinese LIS educational and research focus. First, the Chinese are seeking to get into the best schools possible and create premier universities at home.<sup>121</sup> Second, they are focused with seriousness on science and technology innovation.<sup>122</sup> Third, they are focused on collaboration within and between universities, companies and the Chinese government.<sup>123</sup> The purpose is not to beat us to the top,<sup>124</sup> but to “Leapfrog” beyond Western standards to the next generation of innovation and high-end technology.<sup>125</sup> The design of the LIS is intended to support the development of leading universities and research institutes through competitive advantage and collaboration.<sup>126</sup> Additionally, it is purposed to ensure the success of China's 863 technology policy to achieve core technology advances in military and civilian fields.<sup>127</sup>

---

<sup>119</sup> Interview with Susan Ardis, *supra* note 71.

<sup>120</sup> See HUO ZHONGWEN & WANG ZONGXIAO, *supra* note 54 (providing an overview on Chinese intelligence collection strategies).

<sup>121</sup> FRIEDMAN, *supra* note 98, at 224–25.

<sup>122</sup> *Id.*

<sup>123</sup> *Id.*

<sup>124</sup> *Id.* at 365.

<sup>125</sup> TIMOTHY L. THOMAS, *THE DRAGON'S QUANTUM LEAP: TRANSFORMING FROM A MECHANIZED TO AN INFORMATIZED FORCE* (2009) (discussing the People's Liberation Army new mode of thinking to apply Sun Tzu's concepts in the information age).

<sup>126</sup> See Xue-Ming Bao, *supra* note 99 (discussing the virtual nature of China's National Science and Technology Library).

<sup>127</sup> See *National High-tech R&D Program (863 Program)*, MINISTRY OF SCI. & TECH. OF THE PEOPLE'S REPUBLIC OF CHINA (Jul. 7, 2009), <http://www.most.gov.cn/eng/programmes1/index.htm> (discussing China's National High-tech research and development program as the 863 Program and its objectives (1) to boost innovation capacity in the high-tech sector; to achieve breakthroughs in key technical fields that concern economic lifeline and national security; and, to “leap-frog” development in key high-tech fields to fulfill strategic objectives). This program is aimed at the forefront of world

## XI. COMPETITIVE INTELLIGENCE MISSION

To better understand the Western vulnerabilities of emerging technology development and patent law, one must better understand the Chinese LIS architecture. The LIS architecture by design creates competitive advantage for China's leading research entities against Western innovators. China's NSL and its affiliate libraries include in their mission statement *Competitive Intelligence*—*Jing Zheng Qing Bao*—as a national priority.<sup>128</sup> Before going on its important to define Competitive Intelligence. Typically, Competitive Intelligence is a concept utilized primarily in the commercial sector. It refers to a broad array of research collection and often carries various definitions. With regard to China, the term is characteristic of an aggressive and focused pursuit of commercial competitor information. Indeed, it would appear from a survey of publications in this area that Chinese libraries do not take on a passive role, but rather are actively engaged in the collection of breaking research information.<sup>129</sup> The active collection and databasing of scientific and technology resources is helping drive stupendous growth in patent applications and journal articles.<sup>130</sup>

## XII. DIGITAL EXPLOITATION

The field of Competitive Intelligence itself is trending toward more clandestine intelligence collection and may include elements or naming conventions associated with Market Research Analysis, Business Intelligence, Patent Strategy and Protection, Pre-Competitive Research, Collaborative Research, Due Diligence, Competitor Intelligence, Alerting Services, Early Warning, or Horizon Scanning, etc. All of these collection methods have one

---

technology development and at intensifying innovation efforts to outpace front-runners and "leap-frog" beyond. *Id.* MOST takes the lead in drawing up science and technology plans and policies, drafting related laws, regulations and department rules, and guaranteeing their implementation. *Id.* In 1986, leading Chinese scientists proposed to accelerate China's high-tech development, which later led to the vision and implementation of Program 863. *Id.*

<sup>128</sup> See Zhang Zuozhi George, *supra* note 17 (discussing China's reference to Competitive Intelligence as *Jing Zheng Qing Bao* and the role played by local and national government in its development); see also SUN TZU, *supra* note 1, at 20 ("What the ancients called a clever fighter is one who not only wins, but excels in winning with ease. But his victories bring him neither reputation for wisdom nor credit for courage. For inasmuch as they are gained over circumstances that have not come to light, the world at large knows nothing of them, and he therefore wins no reputation for wisdom; and inasmuch as the hostile state submits before there has been any bloodshed, he receives no credit for courage."). See generally Zhengzhong Li & Yu Dong, *Competitive Intelligence in China: A Case Study*, 8.1COMPETITIVE INTELLIGENCE REV. 73 (1997) (discussing the role of Competitive Intelligence in China).

<sup>129</sup> See Cheng Shuai, *supra* note 43.

<sup>130</sup> Rovner, *supra* note 76.



commonality—digital exploitation of information on a competitor's plans, intentions, and developments. In spite of ethical Competitive Intelligence guidance proffered by organizations such as the Society for Competitive Intelligence Professionals (SCIP),<sup>131</sup> the proliferation of these analytical methodologies and collection techniques, combined with advanced technologies,<sup>132</sup> networking, databasing, analysis, targeted elicitation, and intelligence methodologies, presents an increased collection threat to pre-competitive data—(pre-patented data). When these techniques are State-driven or influenced and low profile in nature, they can be collectively described as Offensive Research Techniques (ORT). They may be overt and legal, but they can be exceptionally damaging to emerging innovation. The Chinese LIS provides a network through which the Chinese government may use low profile ORT in a predatory manner.

### XIII. OFFENSIVE RESEARCH TECHNIQUES (ORT)<sup>133</sup>

The Competitive Intelligence mission of Chinese LIS lines up with Chinese military strategists wide-ranging concept of the battlefield.<sup>134</sup> The LIS mission can be incorporated into a battle planner's *kaleidoscope* to provide an inexhaustible variety of military or quasi military operations in

---

<sup>131</sup> *Vision and Mission Statements*, STRATEGIC & COMPETITIVE INTELLIGENCE PROF., <http://www.scip.org/about/content.cfm?itemnumber=580&navItemNumber=503> (last visited Jan. 11, 2012); *Code of Ethics for CI Professionals*, STRATEGIC & COMPETITIVE INTELLIGENCE PROF., <http://www.scip.org/About/content.cfm?ItemNumber=578&navItemNumber=504> (last visited Jan. 11, 2012).

<sup>132</sup> Numerous resources indicate the trend towards clandestine collection of information in the commercial sector. See Delta Airlines, SKYMALL MAG., Late Spring 2011, at 63 (highlighting the proliferation of collection technologies into the mainstream consumer market); see also ACM IV SEC. SERVICES, SURVEILLANCE COUNTERMEASURES 1–32 (1994) (providing “a serious guide to detecting, evading, and eluding threats to personal privacy”); ACM IV SEC. SERVICES, SECRETS OF SURVEILLANCE vii–14 (1993) (providing “a professional’s guide to tailing subjects by vehicle, foot, airplane, and public transportation”). See generally KATHERINE ALBRECHT & LIZ MCINTYRE, SPY CHIPS 1–13 (2006) (discussing the proliferation of radio frequency identification chips for both public and private sector collection purposes); RICHARD J. HEUER, JR. & RANDOLPH H. PHERSON, STRUCTURED ANALYTIC TECHNIQUES FOR INTELLIGENCE ANALYSIS (2011) (providing an overview of analytical techniques).

<sup>133</sup> See SUN TZU, *supra* note 1, at 32 (quoting *Maneuvering*, “Let your plans be dark and impenetrable as night, and when you move, fall like a thunderbolt”); *id.* at 26 (quoting *Weak Points & Strong*, “O divine art of subtlety and secrecy! Through you we learn to be invisible, through you inaudible, and hence we can hold the enemy’s fate in our hands”); *id.* at 14 (quoting *On Waging War*, “A wise general makes a point of foraging on the enemy”); *id.* at 19 (quoting *Tactics*, “Security against defeat implies defensive tactics; ability to defeat the enemy means taking the offensive”).

<sup>134</sup> See generally Zhang Zuozhi George, *supra* note 17 (providing historical background information on Competitive Intelligence in China).

the digital arena.<sup>135</sup> The Chinese LIS architecture is cloaked in legality. However, both civilian and military researchers have access to its resources. This muddles any Law of Armed Conflict (LOAC) analysis for LIS staff, networks, facilities, or holdings.<sup>136</sup> Given LIS's enabling capabilities, both civil and military researchers may utilize/direct Offensive Research Techniques against Western technology entrepreneurs.

Characteristics of a hostile assault against Western technology research initiative that could lead to dual use military developments include: (1) Predation (parasitical solicitation);<sup>137</sup> (2) Precise Acquisition of Science and Technology Information (not general but to the Nth degree);<sup>138</sup> (3) State Support or Governmental Direction (touching on strategic priorities);<sup>139</sup> (4) Quasi-Legal Elicitation (intrusive in nature);<sup>140</sup> (5) Transferability (applicable to military development);<sup>141</sup> (6) Pivotal Attributes (designed for Leapfrog or Tipping Point manufacture/production);<sup>142</sup> (7) Discreet, Surreptitious, or Deceptive Inquiry/Analysis (e.g. masked by third parties);<sup>143</sup> (8) Disruptive

---

<sup>135</sup> See QIAO LIANG & WANG XIANGSUI, *supra* note 24, at 30 ("While no military thinker has yet put forth an extremely wide-ranging concept of the battlefield, technology is doing its utmost to extend the contemporary battlefield to a degree that is virtually infinite . . . In the wake of the expansion of mankind's imaginative powers and his ability to master technology, the battlespace is being stretched to its limits. Using Addition to Win the Game . . . we need only shake the kaleidoscope of addition to be able to combine into an inexhaustible variety of methods of operation.").

<sup>136</sup> See, e.g., M. McCary, *Battlefield Sunrise: The Legal Status of Renewable Energy Sources Examined Under the Laws of Armed Conflict*, 11 USAFA J. LEG. STUD. 99, 107–09 (2002) (providing an example of LOAC analysis which could be applied to libraries).

<sup>137</sup> *Parasitical Solicitation* is defined by the author as solicitation for information on innovative developments that would/could otherwise disadvantage a researcher.

<sup>138</sup> *Precision* is defined by the author as exploitation of a particular researcher's findings in a very narrow area.

<sup>139</sup> *State-Support or Direction* is defined by the author as governmental funding, sponsorship, or objectives for technological research projects.

<sup>140</sup> *Quasi-Legal Elicitation* is defined by the author as any means of untoward elicitation that would offend the sensibilities of a researcher who may be working on technological projects in pre-competitive phases.

<sup>141</sup> *Transferability* in regards to military application is defined by the author as any technology development that can be used for either a civil or military application.

<sup>142</sup> *Pivotal Attributes* or *Tipping Point* research is defined by the author as that research, which if perfected, would lead to numerous successes in the field or other disciplines creating a synergistic effect in technology advancement. See generally MALCOLM GLADWELL, *THE TIPPING POINT—HOW LITTLE THINGS CAN MAKE A BIG DIFFERENCE* 259 (2001) (discussing *Pivotal Attributes*).

<sup>143</sup> *Discreet/Deceptive/Surreptitious Inquiry or Analysis* is defined by the author as those inquiries or analyses made in a manner which is not transparent, not open, and possibly clandestine in manner.

Development— focused in an emerging or explosive technology field;<sup>144</sup> (9) Targeted Research (manifesting a high degree of advanced knowledge of the researcher and/or research area);<sup>145</sup> (10) Timely and Offensive Approach (inquiry is not coincidental but forward to the point of being intrusive).<sup>146</sup> If a Western researcher encounters queries for research with these characteristics, he should be wary that a prospective collaborator may in actuality be an aggressive competitor.

#### XIV. E-LIBRARY TARGETING TOOLS

The primary predatory pre-competitive collection practices that China LIS uses follow:

Alert Services: It is obvious from official briefings that China uses Horizon Scanning and Early Warning software technology to identify new technology developments and provide breaking Alert Services to customers.<sup>147</sup> In some cases China refers to these alerts as “Signal Lamps”<sup>148</sup> in customer databases.<sup>149</sup> These services are intended to put eyes on target research at the earliest stage possible. The purpose of these services would be to provide a “Tip-Off” which would marshal the entire weight of a research team toward a new innovation.

Subject Librarians: China uses Subject Matter Librarians to marshal resources for customers. The Subject Librarian identifies key topics, forecasts future trends, exploits foreign material, and pushes resources to Chinese research teams.<sup>150</sup> The Subject Matter Librarian's skillset is similar

---

<sup>144</sup> *Disruptive Development* is defined by the author as a breakthrough in technology advancement that would throw a competitor off-balance or disrupt commercial markets.

<sup>145</sup> *Targeted Research* is defined by the author as technological leads confined to very narrow targeted requirements—targeted research may or may not be addressed with precision against a particular researcher but may instead be directed more broadly in scope toward institutions or a group of researchers.

<sup>146</sup> *Timely and Offensive* is defined by the author as any inquiry that would offend the sensibilities of a researcher on the basis of when it was received in light of any pre- competitive developments that are ongoing.

<sup>147</sup> Jinxia Huang, *supra* note 18; see also Liu Xiwen, *supra* note 23 (discussing the use of “Signal Lamps” and “Alert Services” in China's Library Information System).

<sup>148</sup> Chinese strategists have traditionally emphasized “*Signals*” in military doctrine. See SUN TZU, *supra* note 115, at 63 (discussing the importance of changing colors so they will not be recognizable to the enemy); SUN TZU, *supra* note 1, at 33 (discussing “*Signals*” as a means of confusing the enemy).

<sup>149</sup> Jinxia Huang, *supra* note 18; see also Liu Xiwen, *supra* note 23 (discussing the use of “Signal Lamps” and “Alert Services” in China's Library Information System).

<sup>150</sup> See Yafan Song, *Continuing Education in Chinese University Libraries: Issues and Approaches*, 55 LIBRI 21, 21–30 (2005), [www.librijournal.org/pdf/2005-1pp21-30.pdf](http://www.librijournal.org/pdf/2005-1pp21-30.pdf) (providing a statistic of 88,900 Science and Technology librarians as of 1994, and describing new skills and talents for

to a Western Intelligence Officer.<sup>151</sup> Their emerging position is one where they are positioned alongside or directly with the research team they are supporting.<sup>152</sup> Personalized subject services are available at leading university libraries and designed to foster innovation.<sup>153</sup>

Link Analysis. In U.S. military and law enforcement circles, connecting the dots between individuals in a targeted group is simply called "Link Analysis."<sup>154</sup> There exist specific software tools, which graphically display social networks to help better understand individual and organizational structures.<sup>155</sup> Chinese libraries appear to be using these techniques to analyze the intellectual structure of given scientific fields.<sup>156</sup> Otherwise described as "Author Co-Citation Analysis", this type of analysis can be used to pinpoint otherwise undisclosed or discreet working groups.<sup>157</sup> These social

---

university librarians such as digital technology management, foreign language exploitation, deep subject matter expertise, ability to forecast, analyze, and access information accurately and quickly, taking concern for intellectual property, and the ability to communicate well with customers).

<sup>151</sup> *Id.* (explaining that, based on the author's experience, the modern day Chinese librarian carries the same skill-set as Western intelligence officers).

<sup>152</sup> See generally Jinxia Huang, *supra* note 18 (indicating the use of Chinese Subject Matter Librarians and their position on the Forward Edge of the Technological Battlespace); see also Liu Xiwen, *supra* note 23 (indicating the use of Chinese Subject Matter Librarians and their position on the Forward Edge of the Technological Battlespace).

<sup>153</sup> See, e.g., *About Us*, SHANGHAI JIAO TONG UNIV. LIBR., available at <http://www.lib.sjtu.edu.cn/view.do?id=1352> (last visited Jan. 7, 2012) (discussing the goals of the SJTU library).

<sup>154</sup> See Steve Inskeep, *U.S. 'Connects The Dots' to Catch Roadside Bombers*, NPR, Dec. 3, 2010, available at <http://www.npr.org/templates/transcript/transcript.php>; For a discussion of U.S. employment of mathematical models to draw inferences from social networks. Arguably these techniques have proliferated into the realm of Competitive Intelligence for exploitation of pre-competitive business data. More ominously, these techniques can be used to assess what is known about an emerging researcher, who he/she is related to, where and what they have done in the past, and what associations and research projects they are working on.

<sup>155</sup> See IACA Resource Center, INTL ASSOC. OF CRIME ANALYSTS, <http://www.iaca.net/resources.asp?Cat=Software> (last visited Jan. 8, 2012) (describing various analytic tools for link analysis).

<sup>156</sup> See Rulmin Ma, *supra* note 75; Qiao Xiaodong et al., *China National Science and Technology Digital Library (NSTL)*, 16 D-LIB MAG. (May/June 2010), <http://www.dlib.org/dlib/may10/xiaodong/05xiaodong.html> ("The National Science Technology Library processes and analyzes citation information from international journals and conference proceedings, in order to supply domestic web users with comprehensive information mining service."). There is nothing that indicates that the "comprehensive information mining service" is available to foreign (e.g. U.S.) researchers.

<sup>157</sup> Interview with Jonathan Pratter, Foreign & Int'l Law Librarian, Tarlton Law Library, The Univ. of Texas School of Law (Feb. 10, 2011) (noting that co-citation analysis is a very effective means of interpreting journal data. Mr. Pratter has over 25 years of information management experience).

networking techniques can be used to locate leads and target advanced or emerging research of leading innovators.<sup>158</sup> Google Chinese Scholar and Pajek have been discussed as two social networking tools available in China for this type of analysis.<sup>159</sup> The exact tools utilized by the NSL network are undetermined.

Cross-Domain Delivery: Chinese library leadership understands that to be effective in supporting advanced research, resources need to be pushed which cross-over various academic domains. The important characteristic of today's high-technology advances is "integration", where each technology is made up of various technologies to form a technology group.<sup>160</sup> Chinese subject librarians are working on this premise in apparent concert with Chinese military strategists.<sup>161</sup> In cases where a breaking innovation is identified, cross-domain research will be pushed to leading researchers allowing them to better understand the various fields impacted.<sup>162</sup>

Visualization: China LIS is using visualization to map out key technologies and identify trends and analysis.<sup>163</sup> Visualization can be very effective in areas

---

<sup>158</sup> See Noah Shachtman, *How Technology Almost Lost the War: In Iraq, the Critical Networks Are Social — Not Electronic*, WIRED MAG. (Nov. 27, 2007), [http://www.wired.com/politics/security/magazine/15-12/ff\\_futurewar](http://www.wired.com/politics/security/magazine/15-12/ff_futurewar), for a discussion of the U.S. application of information technology tools in "network-centric warfare." According to General David Petraeus, this type of warfare is designed to "transmit data, full-motion video, still photos, images, information. So you can more effectively determine who the enemy is, find them and kill or capture, and have a sense of what's going on in the area as you do it—where the friendlies are, and which platform you want to bring to bear." *Id.* On the battlefield, the U.S. has employed the synergy of technology, software, and social science in Human Terrain Teams (HTTs). *Id.* Comparatively, these same tools are being utilized in the science and technology field to map emerging innovations. *Id.* From a review of Chinese library trends, this Competitor State appears well poised for netcentric warfare in the science and technology field. Although not directly considered a front on the War on Terrorism, General John Abizaid's quote regarding our Enemy may be aptly descriptive: "The enemy is better networked than we are." *Id.*

<sup>159</sup> Rulmin Ma, *supra* note 75.

<sup>160</sup> HUO ZHONGWEN & WANG ZONGXIAO *supra* note 54.

<sup>161</sup> See QIAO LIANG & WANG XIANGSUI *supra* note 24 (discussing the important characteristic of military high technology as "integration").

<sup>162</sup> See, e.g., *Information Services*, NAT'L SCI. LIBR., CHINESE ACAD. OF SCI., <http://www.english.las.cas.cn/rs/is> (last visited Jan. 8, 2012) (highlighting Sci-Tech Novelty Retrieval Center which helps researchers through a literature survey to avoid repetition of scientific research).

<sup>163</sup> See Jinxia Hung, *supra* note 17, at slide 31 (noting the use of visualization technologies for information retrieval within the National Science Library architecture). See generally Liu Yong, Jiang Jing & Zhou Jian, *Competitive Intelligence Service Visualization on Knowledge Discovery*, IEEE XPLORE 203–07 (2010), <http://www.ieee.org/portal/innovate/search/search.html> (providing an overview of the use of

of technology, patent, and trends analysis as well as for Co-Author Citation Analysis.<sup>164</sup> Visualization can help researchers better understand a particular problem-set, or the particular technologies associated with a breaking innovation.<sup>165</sup> Additionally, it can identify new leads.<sup>166</sup> We can expect China's use of visualization to increase as it further perfects its LIS architecture.

Warehousing: China uses both commercial and indigenously produced Digital Library holdings to warehouse collection resources.<sup>167</sup> China is seeking to upgrade its servers and network capacity of its LIS architecture.<sup>168</sup> Warehousing increases the LIS ability to conduct deep dive research.<sup>169</sup>

---

competitive intelligence visualization for knowledge discovery)); Wingyan Chung & Ada Leung, *Supporting Web Searching of Business Intelligence with Information Visualization*, IEEE XPLORE 807–11 (2007),

[http://www.ieee.org/portal/innovate/search/article\\_details.html?article=4427193](http://www.ieee.org/portal/innovate/search/article_details.html?article=4427193) (discussing the usefulness of information visualization).

<sup>164</sup> See Stephen Few, *Visualizing Change: An Innovation in Time-Series Analysis*, SAS & JMP White Paper (2007), available at <http://www.jmp.com/few> (providing a sampling of visualization techniques that can be applied across the science and technology spectra).

<sup>165</sup> See Taotao Sun & Steven A. Morris, *Timeline and Crossmap Visualization of Patents*, PROC. OF WIS 1–11 (H. Kretschmer & F. Havemann eds., 2008) (demonstrating the use of mapping and visualization techniques in the context of patents).

<sup>166</sup> See generally Yang Y et al., *Text Mining and Visualization Tools – Impressions of Emerging Capabilities*, World Patent Information (2008), doi: 10.1016/j.wpi.2008.01.007, <http://dblab.mgt.ncu.edu.tw/%E6%95%99%E6%9D%90/2008%20DM/57.pdf> (discussing the various capabilities of visualization tools).

<sup>167</sup> See CHIEN LIN, *supra* note 66, at 131–32, 195–96 (describing China's use of both indigenous and foreign databases for information retrieval); GONG YITAI, *supra* note 65, at 157; Ben Gu, *supra* note 87 (discussing databasing, digitizing, and warehousing of information by the National Library of China); Qiao Xiaodong et al., *supra* note 156 (providing an overview of China's National Science and Technology Library and describing the NSTL's unified and centralized data storage, data mining, information extraction, and metadata storage responsibilities).

<sup>168</sup> See *New Server for the National S&T Library*, CHINA SCI. & TECH. NEWSLETTER, No. 317 (Dec. 30, 2002),

[http://www.most.gov.cn/eng/newsletters/2003/200411/t20041130\\_17714.htm](http://www.most.gov.cn/eng/newsletters/2003/200411/t20041130_17714.htm) (discussing server upgrades for the National Science and Technology Library (NSTL) which will deliver information through a 1000Mbps high-caliber optic network).

<sup>169</sup> High power computer capabilities are increasing research capabilities for libraries in the science and technology arena. See generally, Chris Anderson, et al., *The Petabyte Age*, WIRED MAG., Jul. 2008, at 106–22 (describing the impact of high-powered computer technology to various disciplines; highlighting the analysis of such information data through visualization; hypothesizing the end of theory; and noting also “Tracking the News” through alerting services and analysis—various applications of these technologies can be easily transferred to Competitive Intelligence methodologies). Compare Michael A. Nielsen, *Simple Rules for a Complex Quantum World*, THE SCI. AM., May 2003, at 25–33 (discussing the emerging discipline of quantum mechanics and information science), with Jia Liu, *Metadata Development in China—Research and Practice*, 10 D-LIB MAG. (Dec. 2004),

Networking: China's LIS architecture relies on a collaborative networking model to exchange and harness resources among libraries.<sup>170</sup> As it is a challenge to determine just how foreign resources are managed, there is little transparency in this area. China is improving its NSL network infrastructure and server capacity.<sup>171</sup>

Deep Web Holdings: China's ability to store both current and historic web information will only improve in the future.<sup>172</sup> Chinese researchers will therefore be able to increase their capability to conduct deep dive research on both authors and their works.<sup>173</sup> Western academics, innovators, and businessmen working on new technologies will have difficulty remaining anonymous amidst Chinese capabilities in this field.<sup>174</sup>

Ultimately, these tools are being used to take the fight to the footnotes of the competitor. Alongside these practices are emerging a new type of librarian.

#### XV. CHINESE LIBRARIANS—BIBLIO WARFARE SPECIALISTS

According to Yafan Song, of Renmin University of China, Library, Haidian, Beijing, China, in a 2005 publication entitled "Continuing Education in Chinese University Libraries: Issues and Approaches", China's libraries were considered to be entering a new educational environment with the expectation and capability to support faculty members that were undertaking academic research at a high level in a variety of subjects and tutoring people with high abilities.<sup>175</sup> The skill-set of Chinese librarians was to include: forecasting, analyses, database management, assessment and acquisition of information, collaboration and networking with researchers, management of digital technology, and reading of foreign documents.<sup>176</sup>

---

<http://www.dlib.org/dlib/december04/liu/12liu.html> (last visited Jan. 7, 2012), and FRIEDMAN, *supra* note 98, at 181 (discussing improvements in search engines and future capabilities).

<sup>170</sup> 170 See Press Release, Thomson Reuters and the Chinese Academy of Science Research Front Analysis Center Jointly Honour China's Contribution to Global Research and Development (May 28, 2008), [http://www.thomsonreuters.com/content/press\\_room/science/265534](http://www.thomsonreuters.com/content/press_room/science/265534) (discussing China's collaborative research work).

<sup>171</sup> See, e.g., *New Server*, *supra* note 168.

<sup>172</sup> See Press Release, *supra* note 170 (discussing China's excellence in research).

<sup>173</sup> See *Deep Web Technologies Paves the Way for China to Join the World Wide Science Alliance*, PR NEWSWIRE, Nov. 24, 2008, [www.highbeam.com/doc/1G1-189647461.html](http://www.highbeam.com/doc/1G1-189647461.html) (describing a powerful federated search engine that allows anyone with internet access to launch a single query across World Wide Science's 375 million pages of scientific and technological holdings).

<sup>174</sup> See Li Xiang-jun et al., *Research of Enterprise Competitive Intelligence Collection System Based on Cross-Language Information Retrieval*, 1 ISECS 601–604 (2009) describing cross-language implementation of Competitive Intelligence tools and methodologies).

<sup>175</sup> Yafan Song, *supra* note 150, at 22–23.

<sup>176</sup> *Id.* at 24–25.

These skills are directly comparable to a Western intelligence analyst.<sup>177</sup> The mission may not be aimed at bombs on target, but it is to obtain the tangible end-result of advancements in either the civil or military technology sector. The aim-point is America's center of gravity—*creativity and innovation*.<sup>178</sup> The end-goal of these subject-matter librarians is to analyze and push resources to more senior researchers regardless of the research mission.<sup>179</sup> According to leading Western academics, there is nothing comparable in the American university system.<sup>180</sup> When it comes to patent strategies, Chinese librarians may appear to be innocuous in nature, but they fulfill the roles of targeting, collection management, and analysis. They are in fact spooks<sup>181</sup> in sheep's clothing.

The specialized Subject Matter Librarian assists the Chinese government in obtaining early warning of a new innovation and quickly devoting personally tailored resources to appropriate science and technology research teams.<sup>182</sup> The effect is to obtain breakthrough on advanced technology and capture

---

<sup>177</sup> Based on Author's own experience in field.

<sup>178</sup> Interview with Susan Ardis, *supra* note 71 (noting that arguably, Americans are more concerned with improving on the current technology rather than taking a risk with new creativity and innovation).

<sup>179</sup> See Jinxia Huang, *supra* note 18, at slides 15, 16, 27 (noting that Chinese librarians are "assigned to various institutes to provide personalized training and consulting and customized information analysis services for research labs and teams." Subject Matter Librarians appear networked to info analysis groups and research and development decision-making bodies.). Compare *Brief Introduction of the Wuhan Branch*, *infra* note 262 (discussing Subject Matter Librarians); Yafan Song, *supra* note 150, at 25 (describing the professional skills and abilities emerging in the Chinese librarian field to include "collaboration with students and other members of the learning community to analyse learning and information needs, and to locate and use the resources that will meet those needs").

<sup>180</sup> *Id.*; Interview with Jonathan Pratter, *supra* note 157.

<sup>181</sup> A Spook is loosely defined by the author in this context as any individual under government employment or influence who is collecting information against national priorities for processing or exploitation in the technical arena.

<sup>182</sup> Subject Matter Librarians appear networked to info analysis groups and research and development decision-making bodies. See Jinxia Huang, *supra* note 18, at slides 15, 16, 27 (noting that Chinese librarians are "assigned to various institutes to provide personalized training and consulting and customized information analysis services for research labs and teams"). Compare *Brief Introduction of the Wuhan Branch*, *infra* note 262 (discussing Subject Matter Librarians); GONG YITAI & G.E. GORMAN, *supra* note 43, at 75–76 (stating that Chinese librarians are involved in scientific research and that "generally speaking, professional titles for librarians [in China] include: Research Librarian, Associate Research Librarian, Librarian, Assistant Librarian, and Clerk. Given the multidisciplinary nature of library services, these titles vary in accordance with the nature of the work. Thus, Librarians engaged in scientific research may have the titles of scientists: Research Professor, Associate research Professor, Assistant Researcher, and Practitioner. On the other hand librarians who look after technological equipment may have engineering titles: Senior Engineer, Engineer, Assistant Engineer, and Technician").



market or government control in a particular field. The LIS's early-stage acquisition of theories, processes, theses, or experiments can spark competitive research domestically and further propel government resources toward numerical superiority necessary for gaining critical development edge.<sup>183</sup> While the American strategy of warfare has always been to capture the high ground,<sup>184, 185</sup> Chinese strategy calls to leverage the library. Incidentally, Chinese librarians are active on all fronts—they are internationally active in both Competitive Intelligence and Library Associations and numerous foreign libraries.<sup>186</sup>

## XVI. THE OYSTER EFFECT

The mission statement of the Chinese National Science Library suggests that the LIS architecture is designed to quickly and quietly acquire details of breaking algorithms, production processes, steps for creative replication, analytical techniques, theories, modified materials, software, testing results, etc. as they come off the printer.<sup>187</sup> Remember, we are discussing ORT, which is overt, legal, precise, and low-profile. While, the effectiveness of China's LIS for national objectives, strategic intelligence, early warning, and science and technology development is unknown, a few extrapolations can be made from its mission. Experts say that China is highly competitive; however, they temper their comments with statements that highly original work is

---

<sup>183</sup> See Reuben F. Johnson, *China Eager for Russian Air Technology—Delegation to Industry Expo Largest*, WASH. TIMES, May 4, 2010, at 8 (discussing targeted collection of technical data on Russian jet-propulsion systems by numerous Chinese delegates "like ants on a march").

<sup>184</sup> See Allen G. Peck, *Airpower's Crucial Role in Irregular Warfare*, AIR & SPACE POWER J. 10–15 (Summer 2007),

<http://www.airpower.au.af.mil/airchronicles/apj/apj07/sum07/sum07.pdf> (discussing airpower's irregular warfare applications in an asymmetric environment and use of aircraft as various collection platforms; comparatively Chinese libraries play a similar role in mapping science and technology landscapes).

<sup>185</sup> The Chinese are seeking to utilize their libraries for information dominance. Cf. WILLIAM C. SHERMAN, *AIR WARFARE 3* (Air University Press 2002) (1926) (discussing the importance of looking forward in warfare and using all new developments); DAVID R. METS, *THE AIR CAMPAIGN* 63 (1999) (advocating simultaneous attacks on all varieties of target sets with the priority going to air superiority and high-tech solutions for dominance on the battlefield).

<sup>186</sup> See CHINESE AM. LIBR. ASS'N (CALA), <http://www.cala-web.org> (last visited Jan. 8, 2012) (describing CALA as an affiliate of the American Library Association (ALA)); see also *Standing Committee*, THE INT'L FED'N OF LIBR. ASS'NS (IFLA), <http://www.ifla.org> (last visited Jan. 8, 2012) (indicating permanent representation by China on the Science and Technology Libraries Section).

<sup>187</sup> See *Information Services*, NAT'L SCI. LIBR., CHINESE ACAD. OF SCI., <http://english.las.cas.cn/rs/> (last visited Jan. 13, 2012) (discussing the information services provided by the library).

still rare.<sup>188</sup> Arguably, China's libraries are facilitating creative research that is neither seen nor heard.<sup>189</sup>

What can be deduced, through secondary material is that Chinese LIS acquires breaking information and pushes it to advanced research teams at leading universities and institutes. Those teams are protected not only by a wall of patents, but a wall of culture, language, government protection, and xenophobia.<sup>190</sup> The end result is *The Oyster Effect*: Chinese libraries obtain a small pebble of information on innovation and capitalize on it with the full weight of its customer research teams. The *Clam-Shell* closes around this innovation and advancements behind the Red Flag are then made in both civil and military arenas at the expense of the original innovator, and with little public awareness by the Western world. *Pearls* of technology are advanced rapidly. Science and technology breakthroughs are then patented or rolled-out for public review at time of competitive advantage.<sup>191</sup> The LIS strategy for development appears well laid out. Let the reader decide how effective this strategy is.

#### XVII. ARCHITECTURE OF CHINA'S NATIONAL SCIENCE LIBRARY.<sup>192,193</sup>

As of mid-2008 the Chinese Academy of Science<sup>194</sup> was actively pursuing a

<sup>188</sup> Rovner, *supra* note 76 (quoting Zhigang Shuai, deputy secretary-general of the Chinese Chemical Society and a chemistry professor at Tsinghua University in Beijing as saying that "[a]mong the patents and papers, very, very few can be regarded as groundbreaking, or the best, or the first in their fields"). Compare SUN TZU, *supra* note 1, at 11 ("Laying Plans—All warfare is based on deception, hence when able to attack, we must seem unable"; Chinese researchers arguably maintain their best research behind Chinese walls), and SUN TZU, *supra* note 115, at 49 (quoting "Strategic Assessments—A military operation involves deception. Even though you are competent, appear to be incompetent. Though effective, appear to be ineffective"), with FRIEDMAN, *supra* note 98, at 367 (noting that "China is focused on overcoming its weaknesses beginning with creative thinking—to match our strengths").

<sup>189</sup> Rovner, *supra* note 76.

<sup>190</sup> China has frequently been characterized as a xenophobic nation. See, e.g., Dennis Van Vranken Hicky, *The Roots of Chinese Xenophobia during Most of the Twentieth Century, Chinese Schools Taught History as a Series of Guo Chi, or National Humiliations Caused by Foreign Powers*, 17.7 WORLD & I, 26–37 (July 2002) (discussing the history of Chinese xenophobia).

<sup>191</sup> See, e.g., HANS JOACHIM FUCHS, *DIE CHINA AG: ZIELMAERKTE UND STRATEGIEN CHINESISCHER MARKENUNTERNEHMEN IN DEUTSCHLAND UND EUROPA* 391 (2007) (noting that commercial gains are often not one by the best products but by the timing of an innovation's deployment into the market).

<sup>192</sup> See *Brief Introduction*, NAT'L SCI. LIBR., CHINESE ACAD. OF SCI., <http://english.las.cas.cn/au/bi/> (last visited Jan. 8, 2012), for an official Chinese profile of the Chinese Academy of Sciences National Science Library.

<sup>193</sup> Chinese LIS is modeled on principles of Sun Tzu's strategy. See SUN TZU, *supra* note 1, at 27 (advocating in *Weak Points & Strong* the strength of a single united (research) body while the enemy must split up into (research) fractions).

national-level digital library system designed to integrate scientific and technological research resources for both universities and federal retrieval.<sup>195,196</sup>

The DL system was to provide active support to intelligence collection practices.<sup>197</sup> As described, Chinese librarians have taken on intelligence functions to include direction, collection, processing, and active support to nationally sponsored researchers. Customers were to be able to use the DL system to develop national strategy, planning, management, intelligence, subject selection, research application, promotion, and development of high-end technology projects.<sup>198</sup> The system was in design as far back as 1996.<sup>199</sup> Its services appear robust, but their effectiveness is undetermined.

The NSL maintains a predatory position as demonstrated by its Competitive Intelligence mission and alert services. This increases the threat to early-stage Western research by providing the foundational support necessary for pre-competitive targeting, copyright infringement, dual-use exploitation, cyber penetration, and intellectual property theft. From an investigative standpoint, even if direct infringement on intellectual property rights is not occurring through the LIS, the nature of Chinese LIS connections masks plans and intentions behind Chinese library acquisitions. LIS early warning capabilities and networked university holdings suggest that NSL incorporates a nation-wide design to capitalize on the sheer number of Chinese researchers to secure competitive advantage for state-influenced actors.

---

<sup>194</sup> CAS maintains a Bureau of High-Tech Research and Development and various academic divisions including physics, chemistry, medicine, earth sciences, information technology and technological sciences. It is affiliated with research institutions, educational institutions, high-tech enterprises, and the National Science Library. It promotes the development of China's high and new technology industries. See *generally About CAS, THE CHINESE ACAD. OF SCI. (CAS)*, <http://www.english.cas.cn/ACAS/> (last visited Jan. 8, 2012) (discussing CAS as a leading academic institution and comprehensive research and development center in natural science, technological science, and high-tech innovation in China).

<sup>195</sup> For general background on the development of China's digital library architecture, see Xihui Zhen, *supra* note 108.

<sup>196</sup> *Id.*; see also Wang Wenqing, *Building the New-Generation China Academic Digital Library Information System (CADLIS): A Review and Prospectus*, 16 D-LIB MAG. (May/Jun 2010), <http://www.dlib.org/dlib/may10/wenqing/05wenqing.print.html> (providing an overview of CADLIS).

<sup>197</sup> Liu Xiwen, *supra* note 23.

<sup>198</sup> *Id.*

<sup>199</sup> See *Introduction, CHINESE DIGITAL LIBR. CONSTRUCTING & VALUE-ADDED SERV.*, <http://www.global.cnki.net/grid20/Aboutcnki/Introduction.htm> (last visited Jan. 8, 2012), for a discussion of Tsinghua University's support for the China National Knowledge Infrastructure Project, a national e-publishing project started in 1996. The project was to include newspapers, dissertations, proceedings, yearbooks, reference books, etc. *Id.* CNKI has greatly boosted the Chinese library systems to go digital and help researchers with their works. *Id.*

Although China's LIS may not be directly considered an intelligence collection entity, it clearly has an intelligence collection mission.<sup>200</sup> It was directed by the Chinese Academy of Sciences and its collection processes and model for integrating holdings was designed to be incorporated into national security planning and science and technology collection and research projects.<sup>201</sup> The Chinese DL is purposed to provide one-stop cross-domain research capabilities for the implementation of nationally-directed scientific projects.<sup>202</sup> Chinese Competitive Intelligence has been characterized as "*astonishingly sophisticated*."<sup>203</sup> But this should be unsurprising given the state-level emphasis placed on the subject.

CAS affiliates were to have access to LIS resources through various networks including the Chinese Academy of Sciences Network (CASnet), the Peking University Network (PUnet), the Tsinghua University Network (TUnet) and the National Science Digital Library Network (CSDL).<sup>204</sup> Other networks were being developed for research entities such as the Shanghai Library and affiliated research institutes.<sup>205</sup> The system was likely to be integrated with most if not all science and technology entities such as China's Ministry of Science and Technology (MOST).<sup>206</sup>

Schematics for CAS LIS networks showed the primary network to be the Chinese Sciences Digital Library (CSDL) where both public and private sector customers could utilize shared resources among universities and the Chinese Academy of Sciences.<sup>207</sup> The network was described as a nation-wide service.<sup>208</sup> The level of access for particular customers such as private researchers versus government employees varied but was otherwise undetermined.<sup>209</sup>

China's Subject Matter Librarians are emerging with special status and trust

---

<sup>200</sup> See Jinxia Huang, *supra* note 18; Liu Xiwen, *supra* note 23 (describing clearly a strategic and tactical intelligence/information role of the Library Information System).

<sup>201</sup> Jinxia Huang, *supra* note 18; Liu Xiwen, *supra* note 23.

<sup>202</sup> Liu Xiwen, *supra* note 23.

<sup>203</sup> See Stephen Miller, *Chinese Host SCIP Members*, 4 CI NEWSWATCH (Sept.–Oct., 2001), <http://www.scip.org/publications/CIMArticleDetail.cfm?ItemNumber=1069> (discussing the sophistication of the Chinese business environment and how advanced Chinese Business Intelligence leadership is without much influence from Western Competitive Intelligence practices).

<sup>204</sup> See Jinxia Huang, *supra* note 18; Liu Xiwen, *supra* note 23 (discussing library networks).

<sup>205</sup> See Liu Xiwen, *supra* note 23 (discussing Shanghai Library's network).

<sup>206</sup> Xihui Zhen, *supra* note 108.

<sup>207</sup> See Jinxia Huang, *supra* note 18; Liu Xiwen, *supra* note 23 (providing schematics for the Library Information System).

<sup>208</sup> Liu Xiwen, *supra* note 23.

<sup>209</sup> See Jinxia Huang, *supra* note 18; Liu Xiwen, *supra* note 23 (providing schematics for the Library Information System).

among China's science and technology community.<sup>210</sup> Their role is not just to maintain resources, but to facilitate new innovations.<sup>211</sup> The exact nature of China's LIS public and private connections is an area ripe for further research. Although Chinese libraries claimed to purchase or develop their own DL holdings, there were indications that holdings were also acquired in a predatory or low- profile manner.<sup>212</sup>

#### XVIII. NATIONAL DIRECTION<sup>213</sup>

The National Science Library's LIS system capitalizes on a China's federated and distributed emphasis on learning.<sup>214</sup> Architecturally, CAS directed a science and technology collection program among university libraries; such libraries include those at Peking University, Tsinghua University, and Shanghai University.<sup>215</sup> These are rising universities seeking reputation as world-class or premier research institutes. Their libraries are also being outfitted with the latest in library technology.<sup>216</sup> Additionally, organizations including the Society for Competitive Intelligence in China (SCIC) and the Chinese Institute for Competitive Intelligence (CICI) appeared to be providing training, education, and resources for the NSL mission.<sup>217 218</sup>

---

<sup>210</sup> See Jinxia Huang, *supra* note 18; Yafan Song, *supra* note 140 (discussing Subject Matter Librarians).

<sup>211</sup> Yafan Song, *supra* note 150.

<sup>212</sup> Interview with Susan Ardis, *supra* note 71 (discussing DL holdings).

<sup>213</sup> See *Brief Introduction*, NAT'L SCI. LIBR., CHINESE ACAD. OF SCI., <http://english.las.cas.cn/au/bi/> (last visited Jan. 8, 2012), for an official Chinese background on the National Science Library.

<sup>214</sup> Rovner, *supra* note 76.

<sup>215</sup> See Jinxia Huang, *supra* note 18; Liu Xiwen, *supra* note 23 (discussing library networks).

<sup>216</sup> See Yuan Zhou, *Catching up with Technology: Recent Developments in Chinese Libraries*, CHINESE AM. LIBR. ASS'N. (CALA), <http://www.cala-web.org/book/export/html/642> (last visited Jan. 8, 2012), for a discussion of library developments at Shanghai Library and implementation of a Horizon Integrated System as well as a tempered look at the networking and technological infrastructure of Chinese libraries. Arguably, China's use of Competitive Intelligence even with a slow information architecture is leading to plenty of commercial and military successes.

<sup>217</sup> See SOC'Y OF COMPETITIVE INTELLIGENCE OF CHINA (SCIC), [www.scic.org.cn](http://www.scic.org.cn) (last visited Jan. 8, 2012) (detailing "The Home of Competitive Intelligence"). China's SCIC website espouses Marxist-Leninist ideology and notes the organization is associated with China's Weapon Industry. *Id.* SCIC provides alert services for various government departments and tracks foreign delegates. *Id.* It reportedly has 400 corporate members and 800 individual members with a staff of 2000. It applies military-intelligence theory to economics theory. *Id.* Library staff are on SCIC's General Committee. *Id.* SCIC claims to be a non-profit organization for everyone involved in creating and managing business knowledge. *Id.*

<sup>218</sup> See CHINA INST. OF COMPETITIVE INTELLIGENCE [www.cichina.org/english/aboutus.org](http://www.cichina.org/english/aboutus.org) (last visited Jan. 8, 2012) (describing this organization as the premier Competitive Intelligence

As of 2011, China's three most prominent national libraries, (branch libraries of its National Science Library), espoused a Competitive Intelligence mission.<sup>219</sup> These include Wuhan, Chengdu, and Lanzhou Libraries.<sup>220</sup> Each of these libraries was aligned with the National Science Library Information System of the Chinese Academy of Sciences.<sup>221</sup> These three universities have a self proclaimed intelligence or competitive intelligence function to support CAS scientific research projects.<sup>222</sup> On their websites, Wuhan and Chengdu Library described their mission focus as the exploitation of foreign acquisitions.<sup>223</sup>

A survey of secondary material shows that these libraries likely incorporate the resources, support, guidance, and direction of CAS subject librarians, digital library holdings, and CAS research tools. They would have a variety of accesses to LIS-datalinked research networks and be subject to national level project directives. Appearances suggest that China is building a national system that will support Chinese researchers identified with high-end or emerging research talent.

The national focus of China's education system combined with its emerging library trends indicates that outstanding Chinese scholars are early- identified as rising stars to assist in national research endeavors. They are then pipelined toward critical scientific and technology collection projects that fall under CAS and NSL technology objectives. They may never be working on a western-style closed-door sensitive program, but they will be clam shelled as *Outliers* through LIS's *Oyster Effect*.<sup>224</sup> In parallel, the LIS architecture will vacuum up early stage international research for digital exploitation by the researchers in the NSL network.<sup>225</sup>

---

training organization in China). CICI holds 15 professional Competitive Intelligence and analysis training seminars across China annually. *Id.*

<sup>219</sup> See *Brief Introduction*, NAT'L SCI. LIBR., CHINESE ACAD. OF SCI., <http://english.las.cas.cn/au/org/> (last visited Jan. 13, 2012) (discussing the library's organization and goals).

<sup>220</sup> *Id.*

<sup>221</sup> *Id.*

<sup>222</sup> *Id.*

<sup>223</sup> CHENGDU BRANCH OF THE NAT'L SCI. LIBR., CHINESE ACAD. OF SCI., <http://english.clas.cas.cn/>

(last visited Jan. 13, 2012); THE WUHAN BRANCH OF THE NAT'L SCI. LIBR., CAS <http://english.whlib.cas.cn/> (last visited Jan. 13, 2012).

<sup>224</sup> See generally MALCOM GLADWELL, *OUTLIERS* 15–68 (2008) (discussing the “Matthew Effect” and “10,000 Hour Rule” which provide hidden advantages and extraordinary opportunities and cultural legacies that allow beneficiaries to work hard, gain success, and make sense of the world in ways others cannot).

<sup>225</sup> See *China and Economic Espionage: Hearing Before the Joint Econ. Comm.*, 105th Cong. (1997) (statement of Mr. John J. Fialka), available at

Since China has been developing an integrated system of digital holdings and a system of scientific research support through data-linked library platforms, Chinese researchers who do not have an intelligence affiliation may have served or still serve as *defacto* collectors for national technology priorities. High-end researchers likely have access to alert services of non-public or advanced research leads, and early warning of Western research developments in their particular specialty area. As a result of this “*Tip Off*” information they may time their international travel to engage in targeted non-public or public dialogues with leading researchers in the field. Discerning whether their work is in a civilian or military field would be a challenge.

As shown, LIS resources can facilitate the low profile targeting of particular Western research, which then would be incorporated into China's national-level reference databases. When CAS-sponsored researchers—specifically students and professors—return to China,<sup>226</sup> with unpublished holdings, specific web or network knowledge, unpublished research, or information that would otherwise be considered by Western standards pre-competitive collaborative data, their material would be subject to further collection, review, analysis, databasing, dataholding, and exploitation by the entire network of subject librarians and their LIS expert customers to include those who have expanded access to information from CAS affiliates.

#### XIX. CULTURED PEARLS

In short, a Chinese scientist's sponsorship or affiliation with CAS allows the Chinese researcher to get-out-in-front of a breaking research development with little or no notice to the U.S. intelligence or research community. The CAS integration of Chinese LIS ensures that Chinese researchers will populate NSL holdings through either witting or unwitting participation in state-directed science and technology objectives. This population of advanced research information creates an in informatics environment where China can foster *Cultured Pearls* and “*Out of the Blue*” technology advances in various scientific fields.<sup>227</sup> Chinese commentators on collection strategy have indicated that 80% of science and technology collection

---

[http://www.fas.org/irp/congress/1997\\_hr/j970617f.htm](http://www.fas.org/irp/congress/1997_hr/j970617f.htm) (discussing Chinese collection of economic secrets as a giant “vacuum cleaner”, its emphasis on student collection, and noting the “spin-on” phenomenon of Chinese learning to make better technology products from the design work “spun off” U.S. technology).

<sup>226</sup> See Rovner, *supra* note 76 (quoting Zhigang Shuai regarding China's investment in human resources and welcoming of expats back home, specifically well-trained scientists who have come from almost every leading rroup in North America, Japan, and Europe).

<sup>227</sup> See generally GLADWELL, *supra* note 224.

is gained from open sources.<sup>228</sup> With the advent of LIS collection trends, this percentage has likely climbed to over 90- 95%.<sup>229</sup> Consequently, the Chinese researcher or scientist can be aiding or abetting a dual-use national-level effort without ever being identified as a counterintelligence threat.<sup>230</sup>

Since these libraries are not openly associated with China's intelligence infrastructure, they appear non-threatening. More importantly, Western researchers and academics, even in lead fields remain little aware of the national collection and targeting focus of Chinese libraries.<sup>231</sup> They do, however, pose both a direct and indirect threat to emerging Western research by sheltering high-end research from prying eyes and providing national-level targeting support to leading research teams. At the same-time, China's scientists, librarians, academics, and librarians, have access to a full array of collaborative learning resources to help further the nation's technological

---

<sup>228</sup> E.g., HUO ZHONGWEN & WANG ZONGXIAO, *supra* note 54 (describing how 80% of technology requirements can be garnered from open source information).

<sup>229</sup> From the author's perspective, 90–95% is a reasonable estimate. This percentage is probably higher if augmented with cyber collection. Cf. Adam Entous, *U.S. Sounds Alarm at China's Military Buildup*, WALL ST. J., Aug. 15, 2010, <http://online.wsj.com/article/SB10001424052748703908704575433933444265178.htm> (discussing cyber intrusions which appear to have originated in China and aimed at exfiltrating information of strategic or military utility); Alex Spillius, *America Prepares for "Cyber War" with China*, TELEGRAPH, Jun. 15, 2007, <http://www.telegraph.co.uk/news/worldnews/1554642/America-prepares-for-cyber-war-with-China.html> (discussing how America's foes are looking at ways of hacking into U.S. networks to glean trade and defense secrets); Bryan Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, U.S.-CHINA ECON. & SEC. REVIEW COMM'N (Oct. 16, 2009), [http://www.uscc.gov/researchpapers/2009/NorthropGrumman\\_PRC\\_Cyber\\_Paper\\_FIN\\_AL\\_Approved%20Report\\_16Oct2009.pdf](http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FIN_AL_Approved%20Report_16Oct2009.pdf) (highlighting in the Executive Summary that China's sophisticated cyber intrusion techniques are complemented by a deep knowledge of targeted networks and ability to sustain activities inside targeted networks both in government and commercial sectors); Martin Beckford, Heidi Blake and Duncan Gardham, *China May Seek to "Control the Internet"*, *US Report on Web Hijack Warns*, TELEGRAPH, Nov. 18, 2010, <http://www.telegraph.co.uk/news/worldnews/asia/china/8143460/China-may-seek-to-control-the-internet-US-report-on-web-hijack-warns.html> ("The redirection of internet traffic [by China] is not just political espionage but the inclusion of data from Dell, IBM, Microsoft, and Yahoo raises concerns around corporate espionage.").

<sup>230</sup> See Harvey Rishikof, *Economic and Industrial Espionage*, NAT'L STRATEGY F. REV. (Spring/Summer 2009),

<http://nationalstrategy.com/NSFReview/SpringSummer2009NSFOnlineJournal/FeatureEssayEconomicandIndustrialEspionage.aspx> (discussing intellectual thieves "eating our lunch" with significant technologies walking out of our laboratories with substantial commercial and substantial defense applications).

<sup>231</sup> Interview with Susan Ardis, *supra* note at 71; Interview with Jonathan Pratter, *supra* note 157.



prowess. Even significant failures can be a topic of high-interest collection as they can provide Chinese researchers with a critical edge to understanding where to apply, and where not to apply, more promising research and development resources.

## XX. CHAIN OF COMMAND

As of early 2010, the National Science Library of the Chinese Academy of Sciences provided the overarching direction to the development and integration of Chinese Library Information Services.<sup>232</sup> According to its website, the three aims of the NSL were to (1) establish channels between resources as well as services and users; (2) develop digital reference work and information literacy education; and (3) develop subject competency information research, analyze subject trends, and find subject research hotspots.<sup>233</sup> Subject librarians of the NSL were to introduce and recommend all kinds of useful resources, service systems, and information tools to meet scientific demands.<sup>234</sup> Additionally, the NSL provided knowledge services for Very Important Person (VIP) users and key research groups according to the needs of research projects or scientists.<sup>235</sup> Their role was to encourage innovation by shorting the distance between the library and the users by going deep into the first line and making connection with scientific customers.<sup>236</sup>

As of early 2010, the Chinese NSL claimed to be linked to at least 89 CAS institutes in 24 cities across China.<sup>237</sup> It provided an interlibrary loan system connecting every CAS institute and connecting to major academic

---

<sup>232</sup> See generally *Information About the National Science Library*, CHINESE ACAD. OF SCI. (Sept. 17, 2009), [http://english.cas.cn/Re/Lib/200909/t20090917\\_39018.shtml](http://english.cas.cn/Re/Lib/200909/t20090917_39018.shtml) (indicating the direction the NSL provided).

<sup>233</sup> See *General Information About the National Science Library*, CHINESE ACAD. OF SCI. (Sept. 17, 2009), [http://english.cas.cn/Re/Lib/200909/t20090917\\_39018.shtml](http://english.cas.cn/Re/Lib/200909/t20090917_39018.shtml) (indicating the aims of the NSL).

<sup>234</sup> See Jinxia Huang, *supra* note 18 (discussing subject librarian services).

<sup>235</sup> See Jinxia Huang, *supra* note 18; Liu Xiwen, *supra* note 23 (discussing VIP and high-level customers of Library Information System services).

<sup>236</sup> Compare DEITCHMAN, *supra* note 5 (discussing aspects of accelerated technology development; arguably there is a need to maintain the edge in such areas as computing hardware and software, materials, aircraft and missiles, fiber optics, superconductivity, directed energy, etc.), with Jinxia Huang, *supra* note 18 (discussing Slides 7–35 which lay out the Chinese system of library information storage).

<sup>237</sup> *CAS Institutes*, CHINESE ACAD. OF SCI., <http://english.cas.cn/CASI/> (last visited Jan. 8, 2012). The Chinese Academy of Sciences frequently changes access to historic web page data so, consequently, the article is based on the late 2010 findings. For an official Chinese overview of its library structure, see *About CAS*, CHINESE ACAD. OF SCI., <http://english.cas.cn/ACAS/> (last visited Jan. 8, 2012).

libraries.<sup>238</sup> It has developed many innovative services and tools, including integrated journal browsing, online reference, subject portals, and remote and mobile authentication.<sup>239</sup> It has also provided full text of Chinese scientific literature.<sup>240</sup>

The NSL was divided into a General Office, an Operational Office, a Collection Development Department, an Information System Department, Department of Subject Information Services, and an Editing and Publishing Center.<sup>241</sup> From a survey of secondary material, this LIS network appeared to incorporate collection from foreign-based institutes, think tanks, and or policy programs.<sup>242</sup> LIS support or connections to quasi-governmental owned companies could not be discounted. And, Chinese research centers appeared to be included in the network.

## XXI. ORGANIZATIONAL STRUCTURE<sup>243</sup>

The following Chinese libraries were identified with the NSL. They all had a Competitive Intelligence mission. As such, these libraries are likely also be associated with developments at SCIC, CICI, leading university libraries, and technology research parks<sup>244</sup> throughout China. Taking into account NSL's self-described mission to provide prompt information services to institutes research groups, labs, individuals, through in-person and virtual connections,<sup>245</sup> these libraries appear to be fully integrated into a system designed to harvest emerging technical information on scientific topics of national concern. The capability of LIS datalinked research networks between these libraries was largely undefined.

Beijing Library (National Library of China):<sup>246,247</sup> The National Library of

---

<sup>238</sup> *Id.*

<sup>239</sup> See generally *Information About the National Science Library*, CHINESE ACAD. OF SCI. (Sept. 17, 2009), [http://english.cas.cn/Re/Lib/200909/t20090917\\_39018.shtml](http://english.cas.cn/Re/Lib/200909/t20090917_39018.shtml) (discussing the Chinese NSL's innovative services).

<sup>240</sup> *Id.*

<sup>241</sup> See Jinxia Huang, *supra* note 18 (discussing the organization of the NSL).

<sup>242</sup> Author makes this deduction from a review of various library descriptions. See, e.g., Xue-Ming Bao, *supra* note 99 (providing an overview of the NSL Chinese model).

<sup>243</sup> See generally *Administration*, CHINESE ACAD. OF SCI., <http://english.cas.cn/Administration/> (indicating the heading "organizational structure").

<sup>244</sup> See generally Hongyi Sun, Wenbin Ni, Joseph Leung, *Critical Success Factors for Technological Incubation: Case Study of Hong Kong Science and Technology Parks*, 24.2 INT'L J. MGMT. (2007) (discussing technology parks).

<sup>245</sup> See, e.g., Xue-Ming Bao, *supra* note 99 (describing NSL's mission).

<sup>246</sup> See NAT'L LIBR. OF CHINA, <http://www.nlc.gov.cn/old/old/newpages/english/situation/index.htm> (last visited Jan. 8, 2012), for an official Chinese profile of the Beijing Library.

<sup>247</sup> See generally Ben Gu, *supra* note 87 (discussing National Library of China's science and

China is briefed as part of the National Science Library architecture.<sup>248</sup> It is described as being a comprehensive research library, a national repository of home publications and a national center of library information networks.<sup>249</sup> The National Library of China not only has the largest collection of Chinese books in the world, but also the biggest collection of materials in foreign languages in the country.<sup>250</sup> Although the National Library of China appears to be focused on historical holdings, it maintains Chinese doctoral dissertations, and digital science and technology holdings.<sup>251</sup> The library is networked to databases with multiple academic institutions including Shanghai and Tsinghua University.<sup>252</sup> The National Library of China appears also to be closely linked to the other three branches of the National Science Library.

Wuhan Library.<sup>253</sup> The Wuhan Branch of the National Science Library carries out decision-making intelligence, academic intelligence, and enterprise Competitive Intelligence research, and has submitted many high quality research reports, and played an important role as a knowledge base and think tank for CAS.<sup>254</sup> Its focus is on advanced energy, advanced manufacturing, and new materials knowledge for CAS innovation.<sup>255</sup>

The Wuhan Branch of the NSL was founded in 1956 as a regional center of documentation and information system of the Chinese Academy of Sciences.<sup>256</sup> Now known as the Wuhan Library (Whlib), Whlib has been making very important contributions to research activities of CAS, and the local development of science and technology and the economy.<sup>257</sup> Whlib is the sub-center of the China Science and Technology Network Information Center (CSTNet) in Southern-Central China and it owns a strong technical force.<sup>258</sup> It integrates walk-in and web-based services 365 days a year, 12.5 hours per day.<sup>259</sup> Whlib is also Whuhan SciTech Project Consulting Center of

---

technology focus).

<sup>248</sup> See NAT'L LIBR. OF CHINA, *supra* note 246.

<sup>249</sup> *Id.*

<sup>250</sup> *Id.*

<sup>251</sup> *Id.*

<sup>252</sup> *Id.*

<sup>253</sup> See *Brief Introduction, THE WUHAN BRANCH OF THE NAT'L SCI. LIBR., CAS*, <http://english.whlib.cas.cn/> (last modified Aug. 20, 2009), for an official Chinese profile of the Wuhan Library.

<sup>254</sup> See *Brief Introduction of the Wuhan Branch, CAS, THE NAT'L SCI. LIBR., CHINESE ACAD. OF SCI.*, <http://english.las.cas.cn/au/org/whb/> (last modified Sep. 14, 2009) (describing the Wuhan Branch).

<sup>255</sup> *Id.*

<sup>256</sup> *Id.*

<sup>257</sup> *Id.*

<sup>258</sup> *Id.*

<sup>259</sup> *Id.*

CAS and the Branch of Sci-Tech Project Consulting Center of Hubei Province.<sup>260</sup> Whlib is the Documentation and Information Center of Donghu Hi-tech Development Zone to take services to Hi-tech zone and enterprises.<sup>261</sup>

Subject librarians of Whlib go to the institutes of CAS in different cities such as Wuhan, Changsha, Guangzhou, Nanjing, Suzhou, Shenzhen, and carry out service for researchers.<sup>262</sup> Whlib has in the past, also played a leading role in databasing for sustainable development and Chinese environment and resource projects.<sup>263</sup>

Chengdu Library:<sup>264</sup> The Chengdu Branch of the National Science Library, aka Chengdu Library, provides strategic intelligence research, subject information study and service, and competition intelligence service for the leadership, bureaus, science and technology innovation bases, and graduate education bases.<sup>265</sup> Chengdu Branch also provides strategic intelligence for local institutes and enterprises, facilitating decision-making, science research, scientific advancement, and sustainable development of society.<sup>266</sup>

The strategic objective of the Chengdu Library is to establish a digital networked information platform, to provide multi-level science and technology literature information service base, information study base, computer network service base, education base of library science and information study, and intellectual property (IP) information service base.<sup>267</sup>

Chengdu Library administrates the Chengdu node of CST and Chengdu Mirror of the National Science and Technology Library.<sup>268</sup> Chengdu Library has developed featured resources such as Nature Medicine Information Portal, Strategic High Technology Innovation Portal, Patent Innovation Portal, and Sichuan Science and Technology Information Sharing Platform.<sup>269</sup> Chengdu Library cooperates with Sichuan University in master education of library science and informatics.<sup>270</sup>

Chengdu Library was founded in 1958 as a regional center of documentation

---

<sup>260</sup> *Brief Introduction of the Wuhan Branch*, *supra* note 254.

<sup>261</sup> *Id.*

<sup>262</sup> *Id.*

<sup>263</sup> *Id.*

<sup>264</sup> See CHENGDU BRANCH, CHINESE ACAD. OF SCI., <http://www.cdb.cas.cn/> (last visited Jan. 8, 2012), for an official Chinese profile of the Chengdu Library.

<sup>265</sup> See *Chengdu Branch*, THE NAT'L SCI. LIBR., CHINESE ACAD. OF SCI., <http://english.las.cas.cn/au/org/cdb/> (last modified Sep. 9, 2009) (describing the Chengdu Branch).

<sup>266</sup> *Id.*

<sup>267</sup> *Id.*

<sup>268</sup> *Id.*

<sup>269</sup> *Id.*

<sup>270</sup> *Id.*

and information system of the Chinese Academy of Sciences.<sup>271</sup> It is now the biggest science library in southwest China and a leading information service and information study center.<sup>272</sup>

Chengdu Library is a member of Online Computer Library Center (formerly the Ohio College Library Center) (OCLC) and cooperates with colleges and agencies from United States, Britain, Germany, Thailand, Russia, and other countries for international academic exchanges.<sup>273</sup>

Lanzhou Library:<sup>274</sup> The Lanzhou Branch of the National Science Library, aka Lanzhou Library of Academia Sinica (LLAS), is otherwise known as a Scientific and Information Center for Resources and Environment of the Chinese Academy of Sciences.<sup>275</sup> Lanzhou Library plays a crucial role in exploiting and utilizing foreign scientific information sources as well as publicizing domestic scientific research achievements.<sup>276</sup>

Lanzhou Library's major tasks are providing appropriate information research and consulting for innovative research of CAS and for the concerned ministries of the nation in multiple disciplines, especially earth sciences, resources, and environmental sciences.<sup>277</sup> Lanzhou Library has participated and chaired at least forty research projects from the National Key Science and Technology Research and Development Program of China.<sup>278</sup> It has important influence on the research of resources, environmental science, earth sciences, global studies, and regional sustainable development.<sup>279</sup>

Lanzhou Library has journal publications on Advances in Earth Sciences, Remote Sensing Technology and Application, Gold Science and Technology, and Natural Gas Geoscience.<sup>280</sup> Lanzhou Library was founded in 1955, and as of 2006 became a branch library of the National Science Library.<sup>281</sup>

National Science and Technology Library: China's National Science and Technology Library is a virtual library created through the collaboration of major

---

<sup>271</sup> *Chengdu Branch*, *supra* note 265.

<sup>272</sup> *Id.*

<sup>273</sup> *Id.*

<sup>274</sup> See *Brief Introduction*, THE LANZHOU BRANCH OF THE NAT'L SCI. LIBR., CAS, <http://english.llas.cas.cn/au/bi/> (last visited Jan. 8, 2012), for an official Chinese profile of Lanzhou Library.

<sup>275</sup> See *Lanzhou Branch Library*, THE NAT'L SCI. LIBR., CHINESE ACAD. OF SCI., <http://english.las.cas.cn/au/org/cdb/> (last modified Sep. 12, 2009) (describing the Lanzhou Branch).

<sup>276</sup> *Id.*

<sup>277</sup> *Id.*

<sup>278</sup> *Id.*

<sup>279</sup> *Id.*

<sup>280</sup> *Id.*

<sup>281</sup> *Lanzhou Branch Library*, *supra* note 275.

national level libraries and information research institutes.<sup>282</sup> Directed by the Ministry of Science and Technology, the NSTL purchases, collects, and develops literature resources in the fields of science and technology, engineering, agriculture, and medicine from both China and around the world.<sup>283</sup> Based on 2004 statistics, NSTL had a strong focus on collecting English language and other Western language conference proceedings, dissertations, and theses.<sup>284</sup> NSTL provides a strong national online document delivery service strengthening science and technology access.<sup>285</sup>

## XXII. OPERATING AREA

The organizational structure of China's National Science Library and its Library Information Systems outlines China's focus on strategic intelligence, emerging technologies, digital holdings, subject matter exploitation, and patent developments.<sup>286</sup> The operating area for these libraries is purely legal.<sup>287</sup> But the state-directed collection and marshaling of early stage research for competitive advantage raises significant questions for patent attorneys. At what stage should Western researchers be defending their research? If an innovation is "*Captured*"<sup>288</sup> before it is publicized, or even in early print, can ownership of the innovation still be maintained? Since we are in a world where more and more information is stored in digital bits and digital holdings,<sup>289</sup> science and technology libraries and their repositories

---

<sup>282</sup> See, e.g., Xue-Ming Bao, *supra* note 99 (displaying Table 1 NSTL Collection Statistics of Abstract Items dated Aug. 16, 2004 and identifying 2,078,805 foreign conference proceedings and 46,667 dissertations and thesis in its inventory). Given NSTL's mission to avoid duplication it is likely that each library networked to China's National Science Library collects dissertations, conferences proceedings, and theses in niche areas to avoid redundancy.

<sup>283</sup> *Id.*

<sup>284</sup> See *id.* (displaying Table 1 NSTL Collection Statistics of Abstract Items dated Aug. 16, 2004 and identifying 2,078,805 foreign conference proceedings and 46,667 dissertations and thesis in its inventory).

<sup>285</sup> See Qiao Xiaodong, *supra* note 156 (providing an overview of China's National Science and Technology Library).

<sup>286</sup> *Id.*

<sup>287</sup> *Id.*

<sup>288</sup> "Captured" is defined by the author in the science and technology research arena, (both in the military and legal sense), as acquiring ownership where no prior ownership existed, for example, with wild animals, mining, and water, or by military action. See BLACK'S LAW DICTIONARY 727 (3d pocket ed. 2006) (defining *Rule of Capture* as "*Property*. The principle that wild animals belong to the person who captures them, regardless of whether they were originally on another person's land").

<sup>289</sup> See, e.g., Christi Fish, *UTSA Opens Nation's First Bookless Library on a University Campus*, UTSA TODAY, Sept. 9, 2010, [www.utsa.edu/today/2010/09/aetlibrary.html](http://www.utsa.edu/today/2010/09/aetlibrary.html) (discussing the University of Texas at San Antonio's bookless Applied Engineering and Technology (AET) Library and the trend to move higher education library collections online which began in October 2000).

will be a part of the operating area for discreet technology surveillance, collection, and exploitation augmented by cyber infiltration.<sup>290, 291</sup>

Thomas L. Friedman addresses some of these issues by asking “how we can build legal barriers to protect an innovator’s intellectual property so he or she can reap the financial benefits and plow those profits into a new invention.”<sup>292</sup> China’s Library Information System appears to provide a State solution to the problem with ORT’s Oyster Effect. State-influenced researchers are encouraged, rewarded,<sup>293</sup> and protected by its LIS. The challenge for Western businessmen, lawyers, and academics is how to increase collaboration in a manner that encourages sharing of the intellectual property required for cutting edge innovation while simultaneously protecting nascent stage advancements from unauthorized theft or cloning.<sup>294</sup> In light of documented cyber threats,<sup>295</sup> licensing works with digital providers cannot be

---

when Kansas State University opened the Fiedler Engineering Library. The UTSA library encourages collaboration among higher engineering students).

<sup>290</sup> See Siobhan Gorman, *China Expands Cyberspying in U.S., Report Says*, WALL ST. J., Oct. 22, 2009, <http://online.wsj.com/article/SB125616872684400273.html> (discussing U.S.- China Economic and Security Review Commission’s finding that China is utilizing cyberspying operations against U.S. corporations and that the Chinese government has likely supported or orchestrated very professional attacks acquiring technical information. The attacks have been targeted at defense information, conducted with extensive reconnaissance, and large scale).

<sup>291</sup> See Mara Hvistendahl, *The China Synbdrome*, POPULAR SCI. (Apr. 23, 2009), <http://www.popsci.com/scitech/article/2009-04/hackers-china-syndrome> (discussing Chinese hackers attacking U.S. companies and government agencies since 1999 and noting the possibility that cyber attacks might be only loosely affiliated with the Chinese government).

<sup>292</sup> FRIEDMAN, *supra* note 98, at 253–55.

<sup>293</sup> See Richard C. Paddock, *Booming China Lures Key Professors Home from U.S.*, AOL NEWS, Sept. 23, 2010, <http://www.aolnews.com/2010/09/23/booming-china-lures-key-professors-home-from-us/> (describing the Chinese government program called the “Thousand Talents” and monetary incentives to encourage Chinese nationals to seek opportunities in China and also noting the goal of jump-starting innovation in science and technology). Returning scientists are referred to as “sea turtles” while part-time returnees are referred to as “sea gulls.” *Id.* Both are treated as national heroes and set up with first-class science and resource support. *Id.* See also FRIEDMAN, *supra* note 98, at 370–71 (discussing China’s focus on the 2004 U.S. Council on Competitiveness National Innovation Initiative Summit, specifically its translation of our report and integration of U.S. findings into its twenty year strategic plan); SUN TZU, *supra* note 1, at 39 (quoting Chia Lin in Variation on Tactics “Entice away the enemy’s best and wisest men, so that he may be left without counselors”).

<sup>294</sup> Interview with Susan Ardis, *supra* note 71 (arguing that there is little transparency in library sharing). While Western institutions are generally open to researchers, the full extent of sharing by China’s National Science Library’s Library Information System appears restricted and unknown). *Id.*

<sup>295</sup> See, e.g., John J. Tkacik, Jr., *Trojan Dragon: China’s Cyber Threat*, EXECUTIVE SUMMARY BACKGROUNDER (Feb. 8, 2008), <http://www.heritage.org/research/reports/2008/02/trojan-dragon-chinas-cyber-threat>

considered a fully secure manner in which to distribute emerging research publications.<sup>296</sup>

### XXIII. PREDATION

By definition, Predation is the act of Preying or Plundering.<sup>297</sup> As of early 2010, numerous open sources manifested various dangers of predatory collection that could likely be associated with Chinese LIS entities including but not limited to: identification and targeting Western academics, Masters and PhD candidates, early warning of pre-competitive Western research; advanced acquisition of emerging scientific theses for dual-use or competitive research and development; exploitation of Western research centers and laboratories; unauthorized textbook translations; unsolicited requests for non-public research data and scientific papers; pursuit of critical software code; identification and collection of breakthrough algorithms; purchase of illegally acquired holdings; direct technical penetration of university or corporate library networks; and targeting of specific Western researchers for access to library holdings.<sup>298</sup>

---

(providing a survey of publicized cyber attacks attributed to China); Shane Harris, *Chinese Hackers Pose Serious Danger to U.S. Computer Networks*, GOV'T EXEC. (May 29, 2008), <http://www.govexec.com/dailyfed/0508/053008nj1.htm> (noting that "Chinese hackers attempt to map the IT networks of [American corporations] on a daily basis" and further describing that "executives from [at least] three Fortune 500 companies, all had document-stealing code planted in their computers while traveling in China. . . . The Chinese make little distinction between hackers who work for the government and those who undertake cyber adventures on its behalf.").

<sup>296</sup> Interview with Susan Ardis, *supra* note 71.

<sup>297</sup> See RANDOM HOUSE WEBSTER'S COLLEGE DICTIONARY 968 (2001) (defining *Predation* as (1)

the act of plundering or robbing; (2) predatory behavior; (3) the capture and consumption of prey).

<sup>298</sup> This assessment of Predation is based on the author's own experience in the legal and intelligence fields and discussion with Western academics and librarians. In these fields, this type of predation often goes unreported to U.S. investigators and is not frequently prosecuted in civil and criminal court because: (1) damages are difficult to assess and prove, (2) party opponents often are hidden behind third party entities, (3) collection is often masked by the guise of academic collaboration, (4) disclosure of invasive collection is often thought to be embarrassing for the victimized individual/entity, and, (5) collection does not meet threshold for legal challenge. See OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE: A REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE, 2009–2011, 2–3 (2011), [http://www.dni.gov/reports/20111103\\_report\\_fecie.pdf](http://www.dni.gov/reports/20111103_report_fecie.pdf) (noting China as a foreign collector and providing a broad outline of "non-cyber" methods of economic espionage to include: Requests for Information, Solicitation or Marketing of Services, Conferences, Conventions, and Trade Shows, Official Foreign Visitors and Exploitation of Joint Research, Foreign Targeting of U.S. Visitors Overseas, and Open Source Information); Micha Springut, Stephen Schlaikjer & David Chen, *China's Program for Science and Technology Modernization: Implications for*



China's LIS resources have magnified the risk of predation.<sup>299</sup> The challenge is operating as a researcher in this environment.

#### XIV. SITUATIONAL AWARENESS

Considering predation, every U.S. student/researcher needs to understand that his or her research may be leveraged into a much wider research initiative once it's documented in a library setting. Every U.S. student/researcher also needs to think of him or herself as competing against every rising Chinese student who could acquire access to his or her material.<sup>300</sup> Furthermore, every U.S. student/researcher needs to look at foreign collaborators as potential competitors in the event they are seeking to push for patent or commercial opportunities.<sup>301</sup> In the area of high-end engineering, Americans must understand that they are at a disadvantage when it comes to Chinese Offensive Research Techniques.<sup>302</sup> After all, China is seeking to lure their nationals home and obtain competitive edge, not pay them to further U.S. business

---

*American Competitiveness*, U.S.-CHINA ECON. & SEC. REVIEW COMM'N (2011), [http://www.uscc.gov/researchpapers/2011/USCC\\_REPORT\\_China's\\_Program\\_forScience\\_and\\_Technology\\_Modernization.pdf](http://www.uscc.gov/researchpapers/2011/USCC_REPORT_China's_Program_forScience_and_Technology_Modernization.pdf) (documenting China's reliance on foreign innovation as a science and technology strategy: "The [Chinese] government does not aim to move out of the way of markets. Rather, the PRC government has become a leader in a technology commercialization drive . . . China's national innovation system struggles to balance its need to utilize foreign sources of technology with a desire to nurture homegrown innovation. Nevertheless the PRC has positioned itself to reap the benefits of global commercial and scientific networks."); Dave Drab, *Economic Espionage and Trade Secret Theft: Defending Against the Pickpockets of the New Millennium*, XEROX WHITE PAPER 4 (2003), [http://www.xerox.com/downloads/wpaper/x/xgs\\_business\\_insight\\_economic\\_espionage.pdf](http://www.xerox.com/downloads/wpaper/x/xgs_business_insight_economic_espionage.pdf) (discussing the danger of foreign governmental collection and outlining various types of information targeted to include financial, organizational, marketing, technical, and scientific data, such as access card control information, project information, pricing information, sales forecasts, financial information, computer source code, test material/prototypes/design specifications, customer business info, engineering plans and drawings, formulas, research, blueprints/diagrams, confidential documents, software, implementation methodology, technical records, biomedical research).

<sup>299</sup> See JAMES GLEICK, *CHAOS—MAKING A NEW SCIENCE* 181–87 (1987) (arguing that Chinese libraries create order from information chaos and are thereby poised to capture innovative pearls for exploitation).

<sup>300</sup> FRIEDMAN, *supra* note 98, at 278.

<sup>301</sup> *Id.* at 353.

<sup>302</sup> See Geoff Colvin, *Desperately Seeking Math and Science Majors*, CNN MONEY (July 29, 2010) [http://money.cnn.com/2010/07/29/news/international/china\\_engineering\\_grads.fortune/index.htm](http://money.cnn.com/2010/07/29/news/international/china_engineering_grads.fortune/index.htm) (discussing Applied Materials challenge in finding high-caliber candidates for its new Solar Technology Center and noting that some of the most advanced research in this high-value, fast growing field is being done in China). By comparison, the fastest-growing college majors in America as of 2007 were in parks, recreation, leisure, and fitness studies, as well as security and protective services. *Id.*

advances.<sup>303,304</sup> To that end, they are creating the mechanisms for legally validating idea theft.

## XXV. RULE OF CAPTURE

Arguably, the Chinese Library Information System is positioned on the juridical battlefield to defend a new *Rule of Capture*.<sup>305</sup> Ideas or innovations may be freely captured in the information wild early in the technology planning stage.<sup>306</sup> As long as the information was openly acquired, even in the most incipient stages, it cannot be considered theft of a *Trade Secret*.<sup>307</sup> Amidst China's library trends, U.S. innovators will not be able to claim their innovations are protected by geographical boundaries or digital licenses. If a larger library network obtains, scans, digitizes, and exploits early-stage theses, papers, or curricula, Rule of Capture suggests that the library's customers should reap the legal rewards.<sup>308</sup> A competitor's advancement of a patent on

---

<sup>303</sup> See *Attracting More Overseas Talent*, CHINA SCI. & TECH. NEWSLETTER, No. 561 (Oct. 10, 2009), [http://www.most.cn/eng/newsletters/2009/200910/t20091010\\_73575.htm](http://www.most.cn/eng/newsletters/2009/200910/t20091010_73575.htm) (discussing China's Ministry of Human Resources and Social Security objective to attract more talented people from overseas, especially high caliber overseas Chinese students). The China Ministry of Human Resources and Social Security will attract overseas talent with three programs (1) more study abroad opportunities; (2) more opportunities for talented people to work in China; and (3) support for high-tech start-ups and innovations. *Id.* The brand name for its student programs is "Chinese Serving China." *Id.*

<sup>304</sup> Paddock, *supra* note 293.

<sup>305</sup> See generally, ERNEST E. SMITH ET AL., INTERNATIONAL PETROLEUM TRANSACTIONS 181–82, 236–38 (1993) (discussing *Rule of Capture* as a means to deny liability for draining another property owners reserves). Comparatively, when applied to juridical warfare, one might say Chinese Library Information Services are positioned to drain pre- competitive information resources for early exploitation by the Competitor State.

<sup>306</sup> See JOHN S. LOWE, OIL & GAS IN A NUTSHELL 9–11 (5th. ed. 2009) (discussing Rule of Capture and early application to wild game).

<sup>307</sup> *Trade Secret* is defined as: A formula, process, device, or other business information that is kept confidential to maintain an advantage over competitors; information— including a formula pattern, compilation, program, device, method, technique, or process—that (1) derives independent economic value, actual or potential from being generally known or readily ascertainable by others who can obtain economic value from its disclosure or use, and (2) is the subject of reasonable efforts, under circumstances to maintain its secrecy. This definition states the majority view, which is found in the Uniform Trade Secrets Act. 2. Information that (1) is not generally known or ascertainable, (2) provides a competitive advantage, (3) has been developed at the plaintiff's expense and is used continuously in the plaintiff's business, and (4) is the subject of the plaintiff's intent to keep it confidential). This definition states the minority view, which is found in the Restatement of Torts § 757 cmt. b (1939). BLACK'S LAW DICTIONARY 727 (3d pocket ed. 2006).

<sup>308</sup> See generally *id.* at 629 (defining *Rule of Capture* as "*Property*. The principle that wild animals belong to the person who captures them, regardless of whether they were originally on another person's land"); ONLINE LAW DICTIONARY,

the basis of data that was pre-competitive in nature cannot be considered illegal.<sup>309</sup> So long as the competitor can prove *First Use* in development and support the position with relevant patent filings, the issue of how "*Tip-Off*" information was collected/exploited becomes irrelevant. With regard to China, the State's use of its Library Information System to draw from a well-spring of technology leads will likely hold sway as a legitimate international norm, even if it creates an unfair advantage for Chinese state-directed/influenced entities.<sup>310</sup> The resultant effect will be an increased difficulty of challenging/defending patents on the juridical battlefield.<sup>311</sup>

#### XXVI. RETRENCHMENT

In comparison to China's LIS, American libraries are in a period of retrenchment.<sup>312</sup> Funding for major university library programs is being cut.<sup>313</sup> Collaboration between libraries is declining.<sup>314</sup> Competitive Intelligence tools for library customers are not provided.<sup>315</sup> And, focus on personalized services

---

<http://law.yourdictionary.com/rule-of-capture> (last visited Jan. 13, 2012) (defining *Rule of Capture* as "(1) Acquiring the ownership of property where there previously was no ownership; thereby, any wild animals captured belong to the person who captures them, regardless of whose property they were upon previously. (2) If the recipient of property displays an intent to take full control of that property and not just pass it on to another, that person captures full rights to that property including the ability to pass it on to his or her heirs"); BARRON'S LAW DICTIONARY 68 (5th ed. 2003) (defining *capture* in both a legal and military sense).

<sup>309</sup> Navarro & Autry, *supra* note 26 (suggesting that an American patent in China is considered merely a blueprint).

<sup>310</sup> Cf. MARK W. JANIS, AN INTRODUCTION TO INTERNATIONAL LAW 157 (3d ed. 1999) (noting that there is no international sovereign to enforce international law). See generally Symposium, *The Air and Missile Warfare Manual: A Critical Analysis*, TEX. INT'L. L.J. (2011) (noting that State practice determines what law is not international law). It is doubtful, however, that China would follow *Stare Decisis of Paquete Habana.*; *The Lola*, 175 U.S. 677 (1900), and pay owners of pre-competitive data profits for LIS captured information.

<sup>311</sup> As official reports indicate, it is already extremely difficult to protect and defend patents against Chinese infringement. U.S. INT'L TRADE COMMISSION, PUB. NO. 4199, CHINA: INTELLECTUAL PROPERTY INFRINGEMENT, INDIGENOUS INNOVATION POLICIES, AND FRAMEWORKS FOR MEASURING THE EFFECTS ON THE U.S. ECONOMY 1 (2010) <http://www.usitc.gov/publications/332/pub4199.pdf>.

<sup>312</sup> Interview with Susan Ardis, *supra* note 71 (discussing the looming loss of funding and digital databases for networked sharing under *TexShare*).

<sup>313</sup> See, e.g., Mary Jackson, *Another View: Why Libraries are Not Expendable*, THE RIVER CITIES SUNDAY TRIBUNE, Feb. 20, 2011, at A4 (discussing Texas legislature's proposed 70 percent cut of library services across the State and increasing reliance on digital holdings); Letter from Lisa Dunham, Smithsonian Inst., Air & Space Mag. Adopt-A-Library Program (June 2011) (on-file with Author) (discussing shortage of funds for libraries across the United States).

<sup>314</sup> Mary Jackson, *supra* note 313.

<sup>315</sup> *Id.*

that might yield the next innovation are virtually non-existent.<sup>316</sup> While larger American corporations in recent past had their own technical libraries designed to map emerging technologies, many private technical libraries have closed under market downturns.<sup>317</sup> Americans, who otherwise proudly call themselves creative risk takers, are in this area demonstrating risk aversion.<sup>318</sup> Most companies and researchers are seeking to improve for profit on the last product rather than find the next innovative solution.<sup>319</sup> This library retrenchment will, unfortunately, lead to a Competitor State such as China, meeting and surpassing us in various technical capabilities.<sup>320</sup> As the civilian world makes additional advances in high-end technology, the various cross-over fields in which military applications can be developed will increase.<sup>321</sup> Retrenchment of our libraries thus limits our ability to respond to a Competitor State's "*out-of-the-blue*" advances and minimizes our ability to deter more hostile acts of aggression.<sup>322</sup> On the other hand, China's use of juridical warfare will provide a powerful tool by which to avoid open conflict with the West and secure strategic technological advantages.

## XXVII. THE VULNERABILITY

Chinese library innovation combined with American library retrenchment creates vulnerability in American deterrence.<sup>323</sup> Although individuals engaged in the world of business activities agree that the Chinese are excellent at espionage,<sup>324</sup> they do not expect to lose their Home Field advantage. Chinese

<sup>316</sup> *Id.*

<sup>317</sup> Interview with Susan Ardis *supra* note 71.

<sup>318</sup> *Id.*

<sup>319</sup> *Id.*

<sup>320</sup> DEITCHMAN, *supra* note 5, at 200; see also John Toon, *Technology Indicators: Move Over U.S.—China to be New Driver of World's Economy and Innovation*, GEORGIA TECH RESEARCH NEWS (Jan. 24, 2008),

<http://www.gtresearchnews.gatech.edu/newsrelease/high-tech-indicators.htm> (describing China as a "powerhouse" and highlighting its consistent gains in all technology indicators).

<sup>321</sup> DEITCHMAN, *supra* note 5, at 207.

<sup>322</sup> Cf. LARRY SCHWEIKART, AMERICA'S VICTORIES—WHY THE U.S. WINS WARS AND WILL WIN THE WAR ON TERROR 132—78 (2006) (stating that "If You Build it, We Will Win," and noting that just as Americans willingly accept good ideas from lower ranks, so, too, has the U.S. military embraced inventions and processes from the private sector, giving it an unprecedented advantage in wartime production), and SUN TZU, *supra* note 115, at 90 (quoting Master Sun on *Formation* "So it is that good warriors take their stand on ground where they cannot lose, and do not overlook conditions that make an opponent prone to defeat."). Unfortunately, without a strong collaborative library infrastructure in the science and engineering field, our ability to field innovations on the battlefield is more limited.

<sup>323</sup> See generally THOMAS C. SCHELLING, THE STRATEGY OF CONFLICT (1980).

<sup>324</sup> See Timothy L. Thomas, *Google Confronts China's "Three Warfares,"* PARAMETERS 111 (Summer 2010) ("People engaged in the world of business activities agree on one thing, the

Library Information Systems provide the venue for which overt, legal, precise, and low-profile collection can be conducted on our turf ultimately resulting in a juridical disadvantage in defending emerging technology developments on the international scene.<sup>325</sup> *"The Chinese utilize any number of espionage tools and establish the rules and regulations that stifle attempts by foreign business to participate as an equal in the Chinese market. This is how the Chinese play the game."*<sup>326</sup> They are, however, taking it one step further in looking to capture validity on the international market. The employment of digital reconnaissance,<sup>327</sup> ORT collection, and self-created databases precludes transparent sharing of holdings.<sup>328</sup>

The libraries provide an example of a pragmatic employment of juridical warfare. In the traditional paradigm of Diplomacy, Intelligence Military and Economics, Chinese Libraries have leveraged all four categories. When used for political profiling, they serve to strengthen diplomacy; when utilized to provide intelligence, they serve to strengthen China's strategic and tactical decision-making capabilities; when utilized to advance a dual-use science and technology advances, they serve to strengthen the military; when utilized to acquire competitive information necessary for patent filings, they provide legitimacy to economic advancements and litigation.<sup>329</sup> By this light, China's LIS serves as a critical enabler for defense strategy.<sup>330</sup> The incorporation of China's rapidly

---

Chinese are excellent at espionage.").

<sup>325</sup> See *id.* at 101–13 (discussing Chinese acts of commercial espionage and use of thorough reconnaissance planning and precision attack on folders using breach teams, collection teams, exfiltration teams, and intermediate staging servers, and also discussing culpability of educational institutions in the collection process and noting that China has played down such collection capabilities).

<sup>326</sup> *Id.* at 111.

<sup>327</sup> See generally *id.* at 101–12 (discussing China's reconnaissance efforts).

<sup>328</sup> Jim Garamone, *China's Military Capabilities Continue to Grow, Report Says*, U.S. DEP'T OF DEF. (Mar. 25, 2009), <http://www.defense.gov/news/newsarticle.aspx?id=53642> (discussing the Military Power of the People's Republic of China and quoting Pentagon Press Secretary Geoff Morrell that "more dialogue and transparency was needed in dealing with Chinese government and military").

<sup>329</sup> See generally Rishikof, *supra* note 2 (discussing juridical warfare). One would be remiss to believe that China does not use pre-emptive litigation as a means to protect its technical acquisitions and developments. See Stuart S. Malawer, *Globalism, Trade, and Virginia*, 59 VIRGINIA LAWYER, Dec. 2010, at 27–32 ("China actively and aggressively uses the litigation process for both domestic and foreign policy purposes . . . it uses the litigation process to contest U.S. trade restrictions and, often, as a response to U.S. actions both in and outside the World Trade Organization.").

<sup>330</sup> Arguably, Chinese science and technology library holdings provide leads and foundational information necessary for more direct and clandestine collection activity; See, e.g., Simon Cooper, *How China Steals U.S. Military Secrets*, POPULAR MECHANICS (July 10, 2009), <http://www.popularmechanics.com/technology/military/news/3319656>

growing Competitive Intelligence industry into the LIS mission makes collection of resources and applications for consumers more effective than American library services.<sup>331</sup>

Chinese libraries are most heavily geared toward collecting and analyzing economic secrets.<sup>332</sup> This is a field where they are “*eating our lunch*.”<sup>333</sup> The majority of LIS collection is not suspicious because it’s done openly and legally. According to leading experts, we are seeing a simultaneous build-up of advanced weaponry in the Asia-Pacific region on a scale and at a speed not seen since the Cold War.<sup>334</sup> Alongside this build-up, we will see China’s armed forces develop and field disruptive military technologies while obfuscating plans and intentions.<sup>335</sup> Chinese military officials have stated that in the world of economic warfare the boundary between war and peace becomes fuzzy.<sup>336</sup>

(discussing how China covert agents “vacuum[ed] up every shred of technology information or hardware that they [could] get their hands on); Peter Grier, *Spy Case Patterns the Chinese Style of Espionage*, THE CHRISTIAN SCI. MONITOR (Nov. 30, 2005), <http://www.intelligencesearch.com/ia092.html> (discussing China’s reliance on a multitude of Chinese students, visiting scientists, and nationals of Chinese heritage to meet national science and technology collection objectives); S. Eugene Poteat, *The Attack on America’s Intellectual Property—Espionage After the Cold War*, THE BENT OF TAU BETA PI 16 (Winter 2001), <http://www.tbp.org/pages/publications/Bent/Features/W01Poteat.pdf> (stating that Chinese intelligence services have seen and understood the change from military competition to worldwide economic competition and have completed the shift in their intelligence requirements accordingly to become masters of economic and industrial espionage).

<sup>331</sup> See generally Bao Changhuo et al., *The Developing Chinese Competitive Intelligence Profession*, 9.4 THUNDERBIRD INTL. BUS. REV. 42–46 (1998) (discussing China’s flourishing competitive intelligence industry and prospects for the future).

<sup>332</sup> Thomas, *supra* note 324, at 103–105.

<sup>333</sup> Rishikof, *supra* note 230, at 4 (discussing intellectual thieves “eating our lunch” with significant technologies walking out of our laboratories with substantial commercial and substantial defense applications).

<sup>334</sup> See Amol Sharma et al., *Asia’s New Arms Race*, WALL ST. J., Feb. 12, 2011, <http://www.online.wsj.com/article/SB10001424052748704881304576094173297995198.html> (discussing the most demanding security situation faced since the Second World War, but stating that China is still far from challenging the U.S. for global military supremacy, and quoting Hu Jintao from early 2011 “We do not engage in an arms race. We are not a military threat to any country—China will never seek to dominate or pursue an expansionist policy.”) Chinese defense spending is up, \$78 billion in 2010 and up \$17 billion from 2001. *Id.* This does not include arms imports or technology research expenditures. *Id.* Michael Schiffer, the Deputy Assistant Secretary of Defense for East Asia has stated that the U.S. does not view China as an adversary. *Id.*

<sup>335</sup> See MILITARY POWER 2009, *supra* note 42, at 51 (discussing the impact of capabilities to allow China to project power to ensure access to resources or enforce claims to disputed territories).

<sup>336</sup> See Thomas, *supra* note 324, at 109–10 (discussing 2009 China Military Science article by

"International commerce and advancing technology have increased the likelihood and opportunity for economic intelligence and industrial espionage."<sup>337</sup> Indeed, boundaries are eroding legally, behaviorally, and electronically.<sup>338</sup> In academic settings, and technology parks, where Western intellectual exchange and technological incubation is most advocated,<sup>339</sup> risk of library enabled ORT will increase.<sup>340</sup>

On a tactical level, key vulnerabilities exist. First, we've said a few times that China's library can serve to bring the full weight of a state-level research team to bear on a Western innovator. Second, ORT can be utilized to indirectly obtain access to critical dual-use research databases by entering into third- institute partnerships. Third, it can obtain advanced leads on government activities and research through close affiliation with libraries chartered under the Federal Depository Libraries Plan. Fourth, it can identify, highlight, and foster targeting of otherwise anonymous or obscure researchers. Fifth, it can exploit both hard-copy and digital collections of public, private, or governmental libraries such as NASA and National Labs. Sixth, it can target data collection at the earliest stage possible.

The tactical battlefield of the future is in the footnotes of the information collected. The industries most vulnerable collection by China's ORT are naturally those that China places priority State interest in. Those industries include: clean energy technology, next generation information technology, bio-technology, high-technology (including aviation, space, manufacturing technology), new energy resources, new materials/nano-technology, and advanced automobile designs.<sup>341</sup> These are the industries that innovators should be concerned about

---

Colonel Long Fangcheng and Senior Colonel Li Decai analyzing comprehensive national power, and noting further that the world economic sector has become a goal for the Chinese).

<sup>337</sup> *Id.*

<sup>338</sup> Rishikof, *supra* note 230, at 2, *see also* FRIEDMAN, *supra* note 98, at 375 ("[T]he main challenge to America today comes from the fact that all the walls are being taken down and other countries can now compete with us much more directly.").

<sup>339</sup> *See, e.g., Fact Sheet: U.S.-China Science and Technology Cooperation—Highlights:32 Years of Collaboration*, U.S. DEP'T OF STATE (Jan. 29, 2011), <http://www.whitehouse.gov/sites/default/files/microsites/ostp/st-fact-sheet.pdf> (describing government-to-government collaboration); Fish, *supra* note 289 (discussing collaboration among engineering students in national libraries); Jonathan Watts, *U.S. and China to Unveil Plan to 'Take Over' Cleantech Market*, THE GUARDIAN, Sept. 9, 2009, <http://www.guardian.co.uk/environment/2009/sep/09/china-us-greentech-plan> (discussing business collaboration on high tech clean-energy projects).

<sup>340</sup> Hongyi Sun et al., *supra* note 244, *see also* Charles Day, *Physics in China*, PHYSICS TODAY, Mar. 2010, at 33–38, <http://www.csupomona.edu/~zywang/day.pdf> (noting that China is utilizing home-grown advances and participation in international projects to increase its science and technology capabilities).

<sup>341</sup> Gregory White, *The 7 Strategic Industries the Chinese Government Loves and Why*

protecting as China speaks boldly on both the means and objectives behind its collection and innovation strategy.

#### XXVIII. IMPACT

When it comes to libraries, China is successfully wielding its Soft Power. Globally it is number two in science and technology publications.<sup>342</sup> Skeptics might say don't worry.<sup>343</sup> However, the United States cannot meet the advancement of technologies described by Defense Secretary Gates quickly and nimbly without marshaling its own library resources for scientific and technological advantage. In a battle-space where technology is fluid, lawfare is state-directed, and libraries maintain deep research capabilities, a full awareness of an enemy's application of information resources is uncertain.<sup>344</sup> Chinese libraries increase the scale of that uncertainty by expanding the access of dual-use science and technology collections to top national researchers at all levels.<sup>345</sup> They provide an additional platform for increasing both the quantity and quality of scientific research.<sup>346</sup>

---

*You Should Too*, BUSINESS INSIDER, Feb. 3, 2011, <http://www.businessinsider.com/the-7-strategic-industries-the-chinese-government-loves-2011-2>, see also *China Triples Spending on Nanotechnology over Past Five Years*, CHINA DAILY.COM, Jan. 12, 2011, [http://www.chinadaily.com.cn/business/2011-01/12/content\\_11834566.htm](http://www.chinadaily.com.cn/business/2011-01/12/content_11834566.htm) (highlighting China's investment of over "5 billion yuan (\$760 million) on research and development of nanotechnology between 2006 and 2010" and quoting Wan Gang, Minister of Science and Technology's ultimate goal of achieving original nanotechnology breakthroughs); *China Outlines Roadmap in Developing Emerging Industries of Strategic Importance*, GOV.CN, Sept. 8, 2011, [http://www.english.gov.cn/201009/08/content\\_1698684.htm](http://www.english.gov.cn/201009/08/content_1698684.htm) (providing an official statement documented by Editor Pliny Han). But see Benjamin Lim & Don Durfee, *Exclusive: China May Cut Spending on Strategic Industries*, REUTERS, July 7, 2011, <http://www.reuters.com/assets/print?aid=USTRE7660XO20110707> (arguing that China does not need to invest in its strategic industries if ORT is paying dividends).

<sup>342</sup> See Ping Zhou & Loet Leydesdorff, *China Ranks Second in Scientific Publications Since 2006*, INT'L SOC. FOR SCIENTOMETRICS & INFORMETRICS NEWSLETTER, No. 13, Mar. 2008, at 7–9 (noting that the Chinese path for development is unique among scientific nations). China's world share of publication has been growing exponentially both in absolute and relative terms. *Id.* China is gaining and other major countries/regions are accordingly losing percentage world shares. *Id.*

<sup>343</sup> See FRIEDMAN, *supra* note 98, at 365 (noting some critics who think that China cannot turn out innovators).

<sup>344</sup> See CENT. INTELLIGENCE AGENCY, NIC 2000-02, GLOBAL TRENDS 2015: A DIALOGUE ABOUT THE FUTURE WITH NONGOVERNMENT EXPERTS (2000)

<http://www.internet.cia/cia/publications/globaltrends2015/index.html> (discussing high stakes national security issues and *Key Uncertainties: Technology Will Alter Outcomes*).

<sup>345</sup> *Id.*

<sup>346</sup> See Yao Changqing, *Development Strategy for High-Quality Science and Technology Journals in China*, 16 D-LIB MAG. (Sept./ Oct. 2010), <http://www.dlib.org/dlib/september10/changqing/09changqing.print.html> (describing China's



The American response should be to actively promote incentives for American researchers to collaborate with each other in an environment protected on U.S. soil and fostered by U.S. law.<sup>347</sup> This Competitor State and its development of networked libraries further an environment where the risk of detection of intellectual property infringement is slight. "[Since] the penalties applied by the courts and administrative authorities are generally low and the climate of widespread piracy favours the infringer, Chinese [intellectual property rights] law tends to be seen as an irrelevance—by both the abuser and abused."<sup>348</sup> The Chinese LIS architecture is positioned to exploit pre-competitive data in a manner, which further undermines patent law. It gives the individual with the best access an advantage rather than the individual with the better innovation. On a state-level, LIS provides an avenue for circumventing or minimizing U.S. strategic advantage in military technology advances.

Since patents are the primary vehicle for protecting technology in most technology based-businesses, there is a need to understand how China's LIS can undermine Western law.<sup>349</sup> Chinese companies are aggressively utilizing Competitive Intelligence to secure the high-ground in the marketplace.<sup>350</sup> China's LIS provides additional support for those market gains and provides legitimacy to any early-stage patent infringement. Even though the basic idea behind the patent system in China is the same as that in the U.S. and the U.K: (in exchange for publishing details of an invention, the state grants the inventor a monopoly over his invention for a period of 20 years), the Chinese government is clearly directing, insulating and protecting technology advancements through

---

Ministry of Science and Technology strategy for improving the quality of Chinese science and technology journals and highlighting a priority on indigenous publications).

<sup>347</sup> See Brendan I. Koerner, *Made in America*, WIRED MAG., Mar. 2011, at 105–09 (discussing the trend of U.S. companies to return manufacturing to U.S. soil). Arguably, current public private sector initiatives such as the Federal Bureau of Investigation's *InfraGard—A Collaboration for National Infrastructure Protection* do not and cannot help American companies and innovators advance high-end technology research. See generally INFRAGARD, <http://www.infragard.net> (last visited Jan. 12, 2012). Such public sector corporate outreach programs are one-sided and only serve to collect national security leads. Therefore, full participation cannot be expected by the private industry, only participation that does not inconvenience corporate initiatives. Additionally, *InfraGard's* Subject Matter Experts do not have the charter or technological background to advise on or facilitate high-end technology advances. Similarly, FBI's student advisories do not provide any indication as to the depth of the threat to emerging American researchers studying abroad or to homebound technology entrepreneurs.

<sup>348</sup> HUNTER RODWELL CONSULTING & ROUSE & CO. INT'L, INTELLECTUAL PROPERTY RIGHTS IN CHINA: A GUIDE FOR UK COMPANIES 1 (2004), <http://www.ipo.gov.uk/ipr-guide-china.pdf>.

<sup>349</sup> See generally *id.* at 7–35.

<sup>350</sup> See FUCHS, *supra* note 191, at 394 (highlighting China's aggressive use of Competitive Intelligence to gain the edge in the German market).

the LIS assembly of technological foreknowledge.<sup>351</sup> If history provides any indication, the competitive nature in which this open technology collection is driven can easily mask more sinister intentions.<sup>352</sup> Rest assured, China will play down its collection capabilities and R&D successes.<sup>353</sup>

#### XXIV. EPILOGUE

The author is a former U.S. Air Force intelligence officer and licensed attorney. The account is consistent with reputable analytical assessments and warfare studies. While the effectiveness of China's reliance on a national-level Library Information System (LIS) for science and technology and intelligence exploitation could not be determined, the nature of the information reviewed suggested that the Chinese libraries' pre-competitive collection practices were ubiquitous, targeted, and competitive in nature. They are focused toward nationally directed civilian-military (dual-use) research applications.<sup>354</sup> The predatory nature of the LIS system appears to undercut legal precepts of innovation and newness as China rapidly furthers its *Great Wall of Patents*.<sup>355</sup> While we cannot prevent juridical warfare,<sup>356</sup> our national response should be (1) to raise awareness of the potential library threat, (2) marshal our own library resources<sup>357</sup> for collaborative edge,<sup>358</sup> and (3)

---

<sup>351</sup> See SUN TZU, *supra* note 115, at 168 (discussing the use of spies and quoting Master Sun as saying that "what enables an intelligent government and a wise military leadership to overcome others and achieve extraordinary accomplishments is foreknowledge").

<sup>352</sup> Cf. LADISLAS FARAGO, *THE GAME OF THE FOXES* 37–40 (1973) (discussing German Competitive Intelligence collection as a precursor to military advancements and armed conflict).

<sup>353</sup> See Miao Qihao, *Presentation: Competitive Intelligence in Peacefully Rising China* (Jan. 17, 2011) (discussing innovation and the evolution of a national Competitive Intelligence infrastructure in China at a Competitive Intelligence Conference in France; specifically playing down China's national competitive intelligence capabilities; separately highlighting Competitive Intelligence as a tool for warfare strategy).

<sup>354</sup> Cf. SUN TZU, *supra* note 115, at 67 (quoting Master Sun on *Planning a Siege* "Therefore those who win every battle are not really skillful—those who render others' armies helpless without fighting are the best of all").

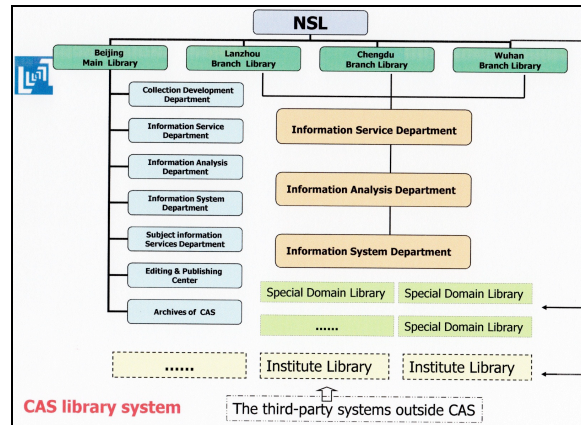
<sup>355</sup> Cf. SUN TZU, *supra* note 1, at 58 ("Rapidity is the essence of war. Take advantage of the enemy's unreadiness, make your way by unexpected routes, and attack unguarded spots.").

<sup>356</sup> Arguably pronouncements, regulations, and laws will not control use of libraries for military purposes. Neither does it appear that such pronouncements have even been fielded; See also Mark Rosenzweig, *Libraries in a Time of War & Emergency*, INT'L RESPONSIBILITIES TASK FORCE, AM. LIBR. ASS'N (Jan. 16, 2011) <http://www.pitt.edu/~ttwiss/irtf/resolutions.war.html> (discussing only the protections of libraries in wartime).

<sup>357</sup> Arguably, science and technology innovation must be advocated at the lowest level of education possible along with concepts of proprietary rights. Cf. Interview with Mary Jackson, Director, Marble Falls City Library, Marble Falls, Texas (Feb. 22, 2011) (discussing the integration of Texas Science Technology Engineering and Math Education programs with local

advocate transparency in China's library developments. We should not fail to define properly our competitor,<sup>359</sup> for the consequences could be stark and irreversible.<sup>360,361</sup>

## APPENDICES



Jinxia Huang on the National Science Library Structure

libraries, but noting the impact of a lack of funding on digital projects).

<sup>358</sup> See MULTIDISCIPLINARY UNIV. RESEARCH INITIATIVE,

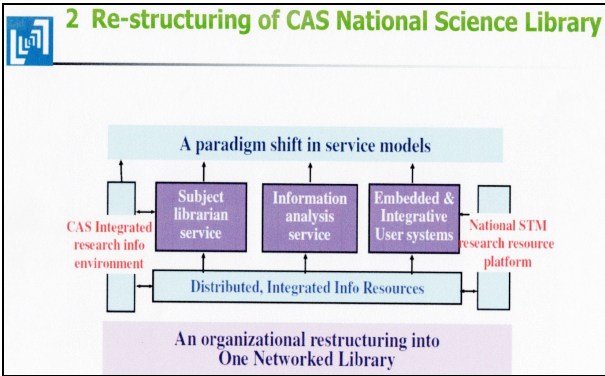
<http://www.arl.army.mil/www/default.cfm?page=472> (last visited Jan. 12, 2012)

(discussing the advantages of a multidisciplinary team effort). Cf. FRIEDMAN, *supra* note 98, at 398 ("Therefore we should be embarking immediately on an all-hands on deck, no holds barred, no budget too large, crash program for science and engineering education."). See generally John Millard, *Ohioview: The Leadership Role of Libraries in Science and Technology Partnerships*, ISSUES IN SCI. & TECH. LIBRARIANSHIP (Winter 2000), <http://www.library.ucsb.edu/istl/00-winter/article4.html> (indicating that some strides have been made in this area but without a full picture of competitor consortia).

<sup>359</sup> See generally John Pomfret, *Insight—China's Attitudes Turn Away from the West*, AUSTIN AM. STATEMENT, Mar. 21, 2010 (discussing China's increasingly anti-Western tone and adoption of policies reflective of heightened fear of foreign influence).

<sup>360</sup> Ambassador Henry A. Crumpton, Keynote Speech at Texas International Law Review Symposium: The Air and Missile Warfare Manual: A Critical Analysis (Feb. 10, 2011).

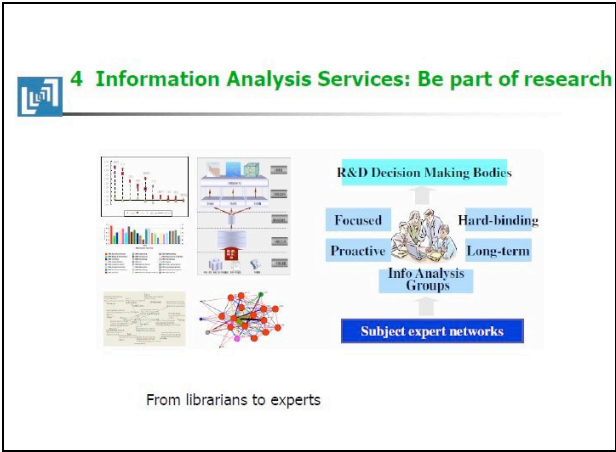
<sup>361</sup> Cf. FRIEDMAN, *supra* note 98, at 398 (quoting Nobel Prize Winning Economist Paul A. Samuelson, MIT, "We may still be the lead cyclist breaking wind for the riders behind us, but the others are closing in.").




Jinxia Huang on Direction of the National Science Library




Jinxia Huang on the National Science Library’s use of Subject Librarians



Jinxia Huang on Targeted National Science Library Services


 **2 Computational & Integrative Informatics**



Emerging Trend Detection  
Scientific Mapping  
Technology Analysis  
Competition Analysis  
Research Profiling  
Policy Profiling  
Literature Based Discovery  
.....  
Computational K-Resources and systems

Data-centric research; Science becomes computational

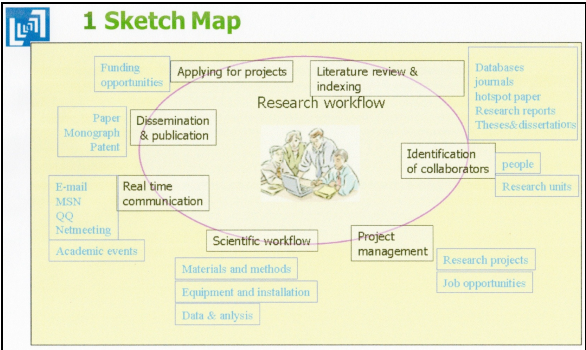
Jinxia Huang on National Science Library’s Intelligence Mission

 **5 Programs Developments in NSL**

**(3) Developments on Intelligence Surveillance and Analysis**

- ✓ **Web resources surveillance and evaluating system**
- ✓ **Scientific Structure Analysis Tool**
- ✓ **Intelligence Analysis Environment**  
To build an virtual environment in which many different data are integrated, shared and co-written by many researchers.

Jinxia Huang on the National Science Library’s Targeted Analytical Cycle



Jinxia Huang Sketch Map



**Law as Shield, Law as Sword: The ICC’s *Lubanga* Decision, Child Soldiers and the Perverse Mutualism of Participation in Hostilities**

*Chris Jenks\**

*The International Criminal Court’s Lubanga decision has been hailed as a landmark ruling heralding an end to impunity for those who recruit and employ children in armed conflict and a pivotal victory for the protection of children. Overlooked amidst this self-congratulation is that the ICC incorrectly applied the law governing civilian participation in hostilities which perversely places child soldiers at greater risk of being attacked. The Court created a false distinction between active and direct participation in hostilities. Expanding the kinds and types of behaviors that constitute children actively participating in hostilities expanded Lubanga’s liability. But under the law of armed conflict active and direct refer to the same quantum of participation. And when a civilian, including a child soldier, directly participates in hostilities, they lose a pivotal protection - the protection from being made the lawful object of attack. The ICC’s first verdict confuses an already opaque area of the law. Worse, the ICC now provides the international legal imprimatur for the permissible targeting of child soldiers under a wider range of circumstances than previously recognized.*

Table of Contents

---

I. INTRODUCTION.....	107
II. BACKGROUND.....	109
III. CHILD SOLDIERS.....	113
A. Age of A Child Soldier Under International Law.....	113
B. Age of of the Child Soldiers in the UPC/FPLC.....	115
C. Activities Lubanga’s Child Soldiers Performed.....	116
D. Parties’ Views on Active Participation.....	117

---

· Assistant Professor of Law and Director, Criminal Justice Clinic, SMU Dedman School of Law.

IV. CIVILIANS UNDER THE LAW OF ARMED CONFLICT.....	119
A. <i>Active vs. Direct Participation</i> .....	120
V. THE LUBANGA DECISION'S RISK TO CHILD SOLDIERS.....	122
VI. CONCLUSION.....	124

## I. INTRODUCTION

On March 14, 2012, the International Criminal Court announced its first ever verdict, finding a Congolese rebel militia leader guilty of conscripting and enlisting child soldiers under the age of fifteen into armed groups and using them to actively participate in hostilities,<sup>1</sup> which are war crimes under the Rome Statute.<sup>2</sup> The Situation in the Democratic Republic of the Congo in the Case of the *Prosecutor v. Thomas Lubanga Dyilo* focused on offenses committed in northeastern Democratic Republic of the Congo (DRC) between 2002 and 2003. This case marked a series of firsts for the International Criminal Court (ICC); the trial flowed from the court's first formal investigation,<sup>3</sup> Lubanga

---

<sup>1</sup> The term child soldiers, while used in this article, is often, and incorrectly, conceptualized as the barefoot boy carrying an AK-47 assault rifle half his size; See generally MARK DRUMBL, REIMAGINING CHILD SOLDIERS IN INTERNATIONAL LAW AND POLICY (2011) (discussing how, contrary to popular conceptions, there are almost as many girl child soldiers as boy child soldiers, how child soldiers perform more support type functions than carry and use weapons, and how there are more child soldiers in south Asia than Africa). The more contemporary, albeit wordy, term is children associated with armed forces and armed groups. UNICEF, The Paris Principles. Principles and Guidelines on Children Associated With Armed Forces or Armed Groups, ¶ 2.1 (Feb. 2007), <http://www.unhcr.org/refworld/docid/465198442.html>, see generally The Secretary-General, Report of the Expert of the Secretary-General: Impact of Armed Conflict on Children, delivered to the General Assembly, U.N. Doc. A/51/306 (Aug. 26, 1996).

<sup>2</sup> *Prosecutor v. Thomas Lubanga Dyilo*, Case No. ICC-01/04-01/06, Judgment (Mar. 14 2012), <http://www.icc-cpi.int/iccdocs/doc/doc1379838.pdf> [hereinafter *Lubanga Judgment*]. The court subsequently sentenced Lubanga to fourteen years in prison. Marlise Simons, *International Criminal Court Issues First Sentence*, N.Y. TIMES, July 10, 2012, available at <http://www.nytimes.com/2012/07/11/world/europe/international-criminal-court-issues-first-sentence.html>.

<sup>3</sup> *Lubanga Case*, COAL. FOR THE INT'L CRIM. CT., <http://www.iccnw.org/?mod=drctimelinelubanga> (last visited Mar. 13, 2013). The conflicts in the DRC are sometimes referred to as the First and Second Congo Wars or as Africa's first world war. The conflicts, however styled, have claimed the lives of over five million people and displaced several million more. The conflicts have involved at least 8 African countries and more than twenty armed groups with varying, and alternating, allegiances and backing; See generally Q&A: *DR Congo Conflict*, BBC, <http://www.bbc.co.uk/news/world-africa-11108589> (last updated Nov. 20, 2012). The Second Congo War technically ended in 2003, but the November 2012 fighting in and around the eastern DRC city of Goma stems in large part from unresolved issues in the earlier conflicts. See Jeffrey Gettleman, *Congo Slips Into Chaos Again As Rebels Gain*, N.Y. TIMES, Nov. 26, 2012, available at <http://www.nytimes.com/2012/11/26/world/africa/as-rebels-gain-congo-again-slips-into-chaos.html>.

was the first person the ICC detained,<sup>4</sup> and Lubanga's trial also marked the first time in international criminal justice that victims were formally recognized as participants in the proceedings and not just as prosecution witnesses.<sup>5</sup>

However, the proceedings were not without controversy. The use of confidentiality agreements, the role of third party intermediaries in witness interviews, and the disclosure (or lack) of exculpatory evidence to the defense are examples of controversial practices adopted by the court.<sup>6</sup> As a result, the trial chamber directed Lubanga's release on two different occasions, of which both decisions were appealed and eventually reversed.<sup>7</sup> Victims, availing themselves of their role as participants, unsuccessfully petitioned the court to supplement the charges against Lubanga to include sexual slavery and cruel/inhumane treatment, and then unsuccessfully appealed the denial.<sup>8</sup>

The *Lubanga* decision has been hailed as a landmark ruling which, according to the United Nations Secretary-General's Special Representative for Children and Armed Conflict, heralds an end to impunity for Lubanga and "those who recruit and use children in armed conflict."<sup>9</sup> The head of the United Nations

---

<sup>4</sup> Press Release, International Criminal Court, First Arrest for the International Criminal Court (Mar. 17 2006), available at [http://www.icc-cpi.int/en\\_menus/icc/press%20and%20media/press%20releases/2006/Pages/first%20arrest%20for%20the%20international%20criminal%20court.aspx](http://www.icc-cpi.int/en_menus/icc/press%20and%20media/press%20releases/2006/Pages/first%20arrest%20for%20the%20international%20criminal%20court.aspx).

<sup>5</sup> Along with that recognition, under the Rome Statute, victims are allowed to present their views and observations to the court. Again, for the first time in international criminal justice, the ICC trial chamber in *Lubanga* ordered reparations for the victims; See also Prosecutor v. Thomas Lubanga Dyilo, Case No. ICC-01/04-01/06, Decisions Establishing the Principles and Procedures to be Applied to Reparations (Aug. 7, 2012), <http://www.icc-cpi.int/iccdocs/doc/doc1447971.pdf>, see generally *Victims and Witnesses*, International Criminal Court, [http://www.icc-cpi.int/en\\_menus/icc/structure%20of%20the%20court/victims/Pages/victims%20and%20witnesses.aspx](http://www.icc-cpi.int/en_menus/icc/structure%20of%20the%20court/victims/Pages/victims%20and%20witnesses.aspx) (last visited Mar. 24, 2013); *Thomas Lubanga Trial: Timeline of Victims' Engagement*, REDRESS, <http://www.redress.org/downloads/ThomasLubangavictimstimeline-140312.pdf> (last visited Mar. 24, 2013); *Lubanga Case - Q & A on ICC Landmark Decision on Reparations for Victims*, REDRESS (Aug. 14, 2012), [http://www.vrwg.org/home/home/post/36-lubanga-case---q--a-on-icc-landmark-decision-on-reparations-for-victims#\\_ftn1](http://www.vrwg.org/home/home/post/36-lubanga-case---q--a-on-icc-landmark-decision-on-reparations-for-victims#_ftn1).

<sup>6</sup> See *Lubanga Case*, *supra* note 3. For example, there were 54 status conferences before the trial started. *Lubanga Judgment*, *supra* note 2, at ¶ 10. The presentation of evidence took place from January 2009 until May 2011. *Id.* at ¶ 11.

<sup>7</sup> See Prosecutor v. Thomas Lubanga Dyilo, Case No. ICC-01/04-01/06, Prosecutions appeal against trial chambers I's oral decision to release Thomas Lubanga Dyilo and Urgent Application for Suspensive Effect (July 2, 2012), <http://www.icc-cpi.int/iccdocs/doc/doc909257.pdf>.

<sup>8</sup> Prosecutor v. Thomas Lubanga Dyilo, Case No. ICC-01/04-01/06, Joint Application of the Legal Representatives of the Victims for the Implementation of the Procedure under Regulation 55 of the Regulations of the Court (May 22, 2009).

<sup>9</sup> In landmark ruling, ICC finds Congolese warlord guilty of recruiting child soldiers, UN NEWS CENTRE (Mar. 14, 2012), available at <http://www.un.org/apps/news/story.asp?NewsID=41537&Cr=ICC&Cr1#.UNGGgYletK>.



Childrens Fund called the decision a “pivotal victory for the protection of children in conflict.”<sup>10</sup> Overlooked amidst this self-congratulation is that the ICC’s first case incorrectly applied the law governing civilian participation in hostilities. Worse, the *Lubanga* Court’s overbroad interpretation of the criminal prohibition against employing children in hostilities leads to child soldiers losing, not gaining, protection under the law of armed conflict.

The criminal prohibition against employing children in hostilities is undoubtedly intended to protect child soldiers. Expanding the kinds and types of behaviors that constitute children actively participating in hostilities expanded the scope of Lubanga’s liability. But, while there is a protective aspect in that expansion, there is a retributive one as well, which is not directed at the Lubangas of the world. When a civilian, including a child, directly participates in hostilities, they lose a pivotal legal protection—the protection from being made the object of attack.

If the question of what constitutes direct participation is asked from a retributive perspective, as in when someone may be targeted, the range of qualifying activities is narrowly subscribed. While the perspective, retributive or protective, shapes the scope of the attendant answer, there is an unavoidable duality. This article explores the perverse mutualism of participation in hostilities, which the *Lubanga* court seemingly ignored.

The first section will review the conflicts in eastern DRC in which Lubanga utilized child soldiers. The next section discusses the lack on international consensus on the age of majority as a backdrop for the difficulties the ICC faced. From there, the article details the types of activities the ICC found UPC/FPLC child soldiers engaged in and the parties’ arguments as whether those activities constituted active participation in hostilities. The focus of the article then illustrates how the court incorrectly parsed active from direct participation. The article concludes that the *Lubanga* Court unfortunately further confused an already opaque area of the law. In the process, the ICC provides the international legal imprimatur for the permissible targeting of child soldiers under a wider range of circumstances than previously recognized.

## II. BACKGROUND

Against the backdrop of “a series of political upheavals and rapidly shifting military alliances” in northeastern DRC that created a humanitarian situation the United Nations called “close to catastrophic”, Lubanga co-founded the Union des Patriotes Congolais (UPC) on September 15, 2000.<sup>11</sup> The UPC then

---

<sup>10</sup> *Id.*

<sup>11</sup> Lubanga Judgment, *supra* note 2, at ¶¶ 79–81 (noting that Lubanga served as the “President” of the UPC).

became a rebel movement that vied for military control of the Ituri district, a mineral rich region of the DRC bordering Uganda.<sup>12</sup> To enable and foster that control, Lubanga mandated that every family in the area "contribute to the war effort by providing a cow, money, or a child" to the UPC.<sup>13</sup>

The UPC took over the city of Bunia, the capital of the Ituri district, on August 9, 2002.<sup>14</sup> This proved to be a turning point in the conflict because the "nature of the violence against the civilian population reached unprecedented extremes."<sup>15</sup> To better facilitate this violence, Lubanga created the military wing of the UPC, the Forces Patriotiques pour la Libération du Congo (FPLC), for which he served as commander in chief.<sup>16</sup> With that:

[t]he need for a more substantial army led to increased recruitment of young people—regardless of age—by targeting schools and the general public, and through coercive campaigns in the villages. . . . this inevitably led to the conscription, enlistment and use of children below 15 years of age . . .

Furthermore, no attempt was made to check the ages of the recruits.<sup>17</sup>

Around this time, Lubanga claimed to have an army of some 15,000 troops.<sup>18</sup> But the UPC/FPLC has been described as an army of children.<sup>19</sup> Estimates are that roughly 40% of the UPC were under the age of eighteen,

---

<sup>12</sup> *Id.* at ¶¶ 22, 67, 81. The Ituri is "fertile and rich in resources such as gold, diamonds, oil, [and] timber." *Id.* at ¶ 71. The Ituri also has one of the world's largest concentrations of coltan, a mineral used in cell phone and laptop batteries. See *Q&A: DR Congo Conflict*, *supra* note 3. Resources form much of the basis for conflict in the DRC, ethnic tensions, exacerbated by colonial rule and arbitrarily set borders, the rest. The DRC has close to 450 different ethnic groups, with 18 different groups in the Ituri alone. Lubanga Judgment, *supra* note 2, ¶ 73.

<sup>13</sup> *DRC: MONUC Denounces Recruitment of Child Soldiers by Lubanga's UPC/RP*, IRIN HUMANITARIAN NEWS AND ANALYSIS AFRICA (Feb. 7 2003), <http://ablefromwww.irinnews.org/Report/41492/DRC-MONUC-denounces-recruitment-of-child-soldiers-by-Lubanga-s-UPC-RP> [hereinafter MONUC].

<sup>14</sup> Lubanga Judgment, *supra* note 2, at ¶ 1084. The DRC national government formed the Ituri Interim Administration in 2003, which recognized Bunia as its capital.

<sup>15</sup> *Id.* at ¶ 543.

<sup>16</sup> *Id.* at ¶¶ 27–28.

<sup>17</sup> *Id.* at ¶ 26, 29. Lubanga orchestrated campaigns to recruit soldiers of all ages, including those below the age of 15 years, who were trained and sent to the front line.

<sup>18</sup> Human Rights Watch, *Ituri: "Covered in Blood," Ethnically Targeted Violence in Northeastern DR Congo* 46 (July 2003) [hereinafter Human Rights Watch], available at <http://www.hrw.org/reports/2003/ituri0703/DRC0703full.pdf>.

<sup>19</sup> *Id.* at 46–47. Lubanga at one point claimed that the United Nations "never notified us that we should not recruit children." MONUC, *supra* note 13. In an interview with Human Rights Watch, Lubanga stated that "the UPC does not have many children under eighteen....we sometimes find children. We don't force anyone. It is just those who come freely." Human Rights Watch, *supra* note 18, at 46–47. Another UPC commander stated that the "underage children were all orphans and that the UPC was looking after them." *Id.*

with some as young as seven-years-old.<sup>20</sup> Observers reported UPC/FPL utilized child soldiers still wearing school uniforms, forcibly “recruiting” the entire 5<sup>th</sup> grade of a school in one town and surrounding a neighborhood and abducting the children in another.<sup>21</sup>

From September 2002 until August 2003, Lubanga directed his forces to complete the conquest of the Ituri.<sup>22</sup> Under Lubanga’s leadership, the UPC massacred, tortured, mutilated and raped civilians in the northeast DRC.<sup>23</sup> In April of 2003, Uganda withdrew its 7000 troops stationed in the Ituri, leaving a little more than 800 UN peacekeepers from Uruguay to protect the region.<sup>24</sup> While the presence of the Ugandan soldiers in the DRC was itself controversial, their absence created a power vacuum which the UPC/FPLC and other armed groups were quick to fill. The resulting violence in and around Bunia was nightmarish, at times male child soldiers, wearing wigs and ball gowns, hacked civilians to death with machetes and then cut out and ate their hearts.<sup>25</sup>

The violence was so extreme that on May 30, 2003, the United Nations Security Council adopted Resolution 1484, authorizing the deployment of an emergency force to Bunia.<sup>26</sup> France led the force, which began deploying to Bunia in mid June 2003.<sup>27</sup> France’s efforts, called “Operation Artemis”, succeeded in stabilizing Bunia and facilitated the transition to a more robust United Nations force by the end of the summer.<sup>28</sup>

Lubanga’s hold on the region lessened considerably, and he left eastern DRC for the capital, Kinshasa. There he purportedly awaited promotion to General in the FARDC, the Congolese Army, a reward promised to militia leaders who disarmed their groups (which the UPC/FPLC hadn’t done) and incorporated them into the FARDC, but the UPC continued fighting in the Ituri.<sup>29</sup> In late February 2005, Lubanga’s forces were involved in the murder of

---

<sup>20</sup> *Id.* at 1

<sup>21</sup> *Id.*

<sup>22</sup> Lubanga Judgment, *supra* note 2, at ¶ 67. By the fall of 2002, the UPC/FPLC was in sufficient control that Lubanga wrote the government of the DRC seeking national recognition and autonomy for the Ituri District. *Id.* at ¶ 25.

<sup>23</sup> Human Rights Watch, *supra* note 18.

<sup>24</sup> *Id.* at 52.

<sup>25</sup> BRYAN MEALER, ALL THINGS MUST FIGHT TO LIVE: STORIES OF WAR AND DELIVERANCE IN THE CONGO (2008) (explaining that the mystical belief that wearing the gown and wigs either gave the wearer invulnerability or protected the underlying child soldier in the event of harm).

<sup>26</sup> S.C. Res. 1484, ¶¶ 3, 7, U.N. Doc. S/RES/1484 (May 30, 2003).

<sup>27</sup> *Operation Artemis: The Lessons of the Interim Emergency Multinational Force*, UNITED NATIONS LOGISTICS BASE (Oct. 2004), <http://pbpu.unlb.org/PBPS/Library/Artemis.pdf>.

<sup>28</sup> *See id.*

<sup>29</sup> Press Release, Department of Public Information, Attacks Against UN Personnel Continued Unabated Throughout 2005, UN Staff Union Says, U.N. Press Release ORG/1457 (May 1, 2006), <http://www.un.org/News/Press/docs/2006/org1457.doc.htm>.

nine Bangladeshi United Nations troops near the town of Kafe.<sup>30</sup> The ambush of the peacekeepers was the deadliest single day for the UN in its operations in the DRC.<sup>31</sup> The United Nations Security Council publically condemned the attack.<sup>32</sup> A week later, United Nations forces in northeastern DRC conducted a combined air and ground assault on the UPC and other militia groups involved in the ambush, killing over 60.<sup>33</sup> In mid march, 2005, the DRC arrested Lubanga in Kinshasa for alleged violations of the DRC military criminal code, including murder, genocide, crimes against humanity and illegal detention.<sup>34</sup>

However, in April, 2004, the DRC had requested that the ICC prosecutor investigate "the situation of crimes within the jurisdiction of the Court allegedly committed anywhere in the territory of the DRC since the entry into force of the Rome Statute, on 1 July 2002."<sup>35</sup> In June, 2004, the ICC prosecutor announced he was opening an investigation of grave crimes allegedly committed in the DRC.<sup>36</sup> In March 2006, the ICC unsealed its indictment of Lubanga and he was immediately transferred to The Hague.<sup>37</sup> The charges

---

<sup>30</sup> *Id.* (describing how the UN troops had been protecting a camp of internally displaced persons from militias, like the UPC, which had been looting belongings from the camp and forcing its occupants to pay taxes).

<sup>31</sup> *Id.*

<sup>32</sup> Press Release, Security Council, Security Council Condemns Murder of Nine UN peacekeepers in Democratic Republic of Congo, U.N. Press Release SC/8327/Rev.1\* (Feb. 3, 2005), <http://www.un.org/News/Press/docs/2005/sc8327.doc.htm>.

<sup>33</sup> *U.N. Forces Kill 60 Congo Militia*, CNN INT'L (Mar. 4 2005), <http://edition.cnn.com/2005/WORLD/africa/03/02/congo.deaths>.

<sup>34</sup> *Thomas Lubanga and the ICC*, INT'L CTR. FOR TRANSITIONAL JUST. (2008), [http://humansecuritygateway.com/documents/ICTJ\\_DRC\\_Luganda\\_Factsheet.pdf](http://humansecuritygateway.com/documents/ICTJ_DRC_Luganda_Factsheet.pdf).

<sup>35</sup> Press Release, Int'l Criminal Court, Prosecution Receives Referral of the Situation in the Democratic Republic of Congo (2004), *available at* [http://www.icc-cpi.int/en\\_menus/icc/press%20and%20media/press%20releases/2004/Pages/prosecutor%20receives%20referral%20of%20the%20situation%20in%20the%20democratic%20republic%20of%20congo.aspx](http://www.icc-cpi.int/en_menus/icc/press%20and%20media/press%20releases/2004/Pages/prosecutor%20receives%20referral%20of%20the%20situation%20in%20the%20democratic%20republic%20of%20congo.aspx). The DRC's self-referral was one step ahead of the ICC initiating an investigation under its own authority. In July, 2003, the ICC prosecutor announced he was "closely follow[ing] the situation in the DRC" after having received communications from a wide range of individuals and non-government organizations on events in the Ituri District. *Id.* By August, 2003, "the Prosecutor informed the Assembly of States Parties that he would be prepared to seek authorization from a Pre-Trial Chamber to start an investigation under his proprio motu powers, but that a referral and active support from the DRC would facilitate the work of the Office of the Prosecutor." *Id.*

<sup>36</sup> Press Release, Int'l Criminal Court, The Office of the Prosecutor of the International Criminal Court Opens its First Investigation (June 23, 2004), *available at* [http://www.icc-cpi.int/en\\_menus/icc/press%20and%20media/press%20releases/2004/Pages/the%20office%20of%20the%20prosecutor%20of%20the%20international%20criminal%20court%20opens%20its%20first%20investigation.aspx](http://www.icc-cpi.int/en_menus/icc/press%20and%20media/press%20releases/2004/Pages/the%20office%20of%20the%20prosecutor%20of%20the%20international%20criminal%20court%20opens%20its%20first%20investigation.aspx) [hereinafter Investigation Press Release].

<sup>37</sup> *Democratic Republic of Congo: Situations and Cases*, INT'L CRIM. CT., [http://www.icc-cpi.int/en\\_menus/icc/situations%20and%20cases/situations/situation%20icc%200104/Pages/s](http://www.icc-cpi.int/en_menus/icc/situations%20and%20cases/situations/situation%20icc%200104/Pages/s)

were confirmed and followed by a trial. In announcing its investigation into the DRC, the ICC stated that:

[m]illions of civilians have died as a result of conflict in the DRC since the 1990's.... States, international organizations and non-governmental organizations have reported thousands of deaths by mass murder and summary execution in the DRC since 2002. The reports allege a pattern of rape, torture, forced displacement and the illegal use of child soldiers.<sup>38</sup>

It was Lubanga's recruitment, forcible and otherwise, and use, of child soldiers, which became the basis of the charges against him. Specifically, the ICC prosecuted Lubanga on charges that he, as a co-perpetrator, enlisted and conscripted children under the age of fifteen years into the FPLC and used them to participate actively in hostilities within the meaning of article 8(2)(e)(vii) of the Statute from early September 2002 to 2 June 2003.<sup>39</sup>

These charges required the prosecutor to prove, among other elements, that (1) children under the age of fifteen (2) actively participated in hostilities.

### III. CHILD SOLDIERS

#### A. *Age of A Child Soldier Under International Law*

The Rome Statute's fifteen-year age threshold for criminalizing the enlistment, conscription, and active use in hostilities is unambiguous. But a brief survey of the lack of consensus on the age of majority as applied to service in the military underscores some of the difficulties the Lubanga Court faced. Additional Protocol I (AP I) to the Geneva Conventions states a qualified limitation that "[t]he Parties to the conflict shall take all feasible measures in order that children who have not attained the age of fifteen years do not take a direct part in hostilities"<sup>40</sup> The commentary to that section of AP I makes clear that the age limitation is aspirational and that child soldiers under the age of 15

---

ituation%20index.aspx (last visited Mar. 24, 2013).

<sup>38</sup> Investigation Press Release, *supra* note 38.

<sup>39</sup> See *Situation in the Democratic Republic of Congo in the Case of the Prosecutor v. Thomas Lubanga Dyilo*, INT'L CRIM. CT. (Jan. 29, 2007), <http://www.iccpi.int/iccdocs/doc/doc266175.PDF>; Rome Statute of the International Criminal Court, art. 8(2)(e)(vii), July, 1, 2002, U.N. Doc. A/CONF.183/9\* (prohibiting "[c]onscripting or enlisting children under the age of fifteen years into the national armed forces or using them to participate actively in hostilities," not of an international character).

Lubanga was also charged with violating article 25(3)(a) of the Rome Statute, which deals with modes of liability, specifically individual criminal responsibility. Rome Statute of the International Criminal Court, art. 25(3)(a), July, 1, 2002, U.N. Doc. A/CONF.183/9\*.

<sup>40</sup> Protocol Additional to the Geneva Conventions of 12 Aug. 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, art. 77(2), 1125 U.N.T.S. 17512 [hereinafter AP 1].

were still, reluctantly, if not accepted then expected.

Participation of children and adolescents in combat is an inhumane practice and the ICRC considered that it should come to an end because it entails mortal danger for the children themselves. Nevertheless, the ICRC proposals encountered some opposition, as on this point governments did not wish to undertake unconditional obligations. In fact, the ICRC had suggested that the Parties to the conflict should "take all necessary measures", which became in the final text, "take all feasible measures." Although the obligation to refrain from recruiting children under the age of fifteen remains, the one of refusing their voluntary enrolment is no longer explicitly mentioned. In fact, according to the Rapporteur, Committee III noted that sometimes, especially in occupied territories and in wars of national liberation, it would not be realistic to totally prohibit voluntary participation of children under fifteen.<sup>41</sup>

Additional Protocol II (AP II) to the Geneva Conventions speaks more definitively, that "children who have not attained the age of fifteen years shall neither be recruited in the armed forces or groups nor allowed to take part in hostilities."<sup>42</sup>

The 1990 Convention on the Rights of the Child replicates AP I, requiring feasible measures to prevent persons under the age of fifteen from participating in hostilities.<sup>43</sup> The 2002 subsequent Optional Protocol, which specifically addressed the involvement of children in armed conflict, while using the same feasible measures language, increased the age persons under eighteen.<sup>44</sup>

Under the 1997 Cape Town Principles, the term child soldier means any person under 18 years of age who is part of any kind of regular or irregular armed force or armed group in any capacity, including but not limited to cooks, porters, messengers, and those accompanying such groups, other than purely as family members. It includes girls recruited for sexual purposes and forced

---

<sup>41</sup> AP I, *supra* note 42, at cmt. 3183-84.

<sup>42</sup> Protocol Additional to the Geneva Conventions of 12 Aug. 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, art. 4(3)(c), 1125 U.N.T.S. 17513 [hereinafter AP II].

<sup>43</sup> Convention on the Rights of the Child, art. 38(2), Nov. 20, 1989, 28 I.L.M. 1448 ("States Parties shall take all feasible measures to ensure that persons who have not attained the age of fifteen years do not take a direct part in hostilities."), *see also* Jo de Berry, *Child Soldiers and the Convention on the Rights of the Child*, 575 ANNALS OF THE AMERICAN ACADEMY OF POLITICAL AND SOCIAL SCIENCE 92, 92-105 (2001).

<sup>44</sup> Optional Protocol to the Convention on the Rights of the Child on the Involvement of Children in Armed Conflict, G.A. Res. 54/263, U.N. Doc. A/RES/54/263, art. 1(May 25, 2005) ("States Parties shall take all feasible measures to ensure that members of their armed forces who have not attained the age of 18 years do not take a direct part in hostilities."), *available at* <http://www.unhcr.org/refworld/docid/47fdfb180.html>.

marriage. It does not, therefore, only refer to a child who is carrying or has carried arms.<sup>45</sup>

Ten years later, the 2007 Paris Principles shifted to the term “child associated with an armed forces or armed group,” which was defined as any person below eighteen years of age who is or who has been recruited or used by an armed force or armed group in any capacity, including but not limited to children, boys and girls, used as fighters, cooks, porters, messengers, spies or for sexual purposes.”<sup>46</sup>

As the commentary to AP II aptly summarized “[t]he moment at which a person ceases to be a child and becomes an adult is not judged in the same way everywhere in the world. Depending on the culture, the age may vary between about fifteen and eighteen years.”<sup>47</sup> While the Rome Statute’s use of fifteen years as the child soldier threshold is seemingly unambiguous, determining age of child soldiers is anything but.

#### B. *Age of the Child Soldiers in the UPC/FPLC*

It was tragically self-evident that children serving in the UPC/FPLC at the time. Witnesses testified about how the child soldiers would play childhood games, and about how the female child soldiers would braid grass “as if they [were] braiding the hair of a doll.”<sup>48</sup> In fact, the lack of adult attitudes and demands were some of the perceived advantages of using child soldiers. They were not very demanding, they were not asking for money to buy what they wanted, they didn’t have a girlfriend, they couldn’t drink, whereas older young soldiers had other troubles as well. A child—as long as he can wash and eat, that’s all he needs, while adults, elder soldiers, want more than that.<sup>49</sup>

Determining the age of the child soldiers in the UPC/FPLC proved challenging for the court. The court explained that “[g]iven the undoubted differences in personal perception as regards estimates of age and, most particularly in the context of this case, the difficulties in distinguishing between young people who are relatively close to the age of fifteen (whether above or below), the Chamber has exercised caution when considering this evidence.”<sup>50</sup>

---

<sup>45</sup> UNICEF, Cape Town Principles and Best Practices (Feb. 1997), [http://www.unicef.org/emerg/files/Cape\\_Town\\_Principles\(1\).pdf](http://www.unicef.org/emerg/files/Cape_Town_Principles(1).pdf).

<sup>46</sup> UNICEF, The Paris Principles, Principles and Guidelines on Children Associated With Armed Forces and Armed Groups, ¶ 2.1 (Feb. 2007), <http://www.unhcr.org/refworld/docid/465198442.html> (stating that while a number of countries have signed the Paris Principles, the signatories include some of the worst child soldier offenders, Sudan, Chad, Uganda and the Democratic Republic of Congo).

<sup>47</sup> AP II, *supra* note 44, at cmt. 4549.

<sup>48</sup> Lubanga Judgment, *supra* note 2, at ¶ 807.

<sup>49</sup> *Id.* at ¶ 845.

<sup>50</sup> *Id.* at ¶ 643.

The court considered witnesses from international and non-governmental organizations, both prosecution and defense witnesses, and also video evidence.<sup>51</sup>

While agreeing with the defense that it is difficult to distinguish between a twelve or thirteen-year-old and a fifteen or sixteen-year-old, the court found that photographic and video extracts depicted children “who are clearly under the age of 15.”<sup>52</sup> Even a defense witness affirmatively declined to testify that the UPC did not utilize child soldiers, stating “one can’t exclude that some might have got through the net. When you go fishing, you can have a certain net and some fish can get through ....”<sup>53</sup> Ultimately, the trial chamber held that even allowing for a wide margin of error in assessing an individual’s age, ...it is feasible for non-expert witnesses to differentiate between a child who is undoubtedly less than 15 years old and a child who is undoubtedly over 15. Furthermore, the sheer volume of credible evidence relating to the presence of children below the age of 15 within the ranks of the UPC/FPLC has demonstrated conclusively that a significant number were part of the UPC/FPLC army.<sup>54</sup>

### C. *Activities Lubanga’s Child Soldiers Performed*

Having established that Lubanga and the UPC/FPLC utilized children under the age of the fifteen, willing and unwilling, the next inquiry is whether the activities the children performed constituted active participation in hostilities. The trial chamber found that Lubanga recruited and utilized child soldiers as young as eight-years-old<sup>55</sup> for a variety of functions<sup>56</sup> including fighting in battles, serving as bodyguards,<sup>57</sup> military guards,<sup>58</sup> escorting high ranking UPC/FPLC officials<sup>59</sup> and performing domestic work.<sup>60</sup> Under Lubanga’s leadership, the UPC/FPLC even formed a specific unit of small children, or

---

<sup>51</sup> *Id.* at ¶ 643. The evidence included logbooks from demobilization centers and logbooks, correspondence and reports from the UPC/FPLC. *Id.* at ¶¶ 733, 741, 749, and 753.

<sup>52</sup> *Id.* at ¶ 644. The defense claimed it was “impossible to reliably distinguish “ between children whose ages were 1-2 years on either side of the 15 year threshold.

<sup>53</sup> *Id.* at ¶ 768.

<sup>54</sup> *Id.* at ¶ 643.

<sup>55</sup> *Id.* at ¶ 765. The UPC recruited 8 year olds in 2000, which is prior to the Rome Statute entering force. The youngest age of a UPC child soldier during the timeframe at issue, 2002 to 2003, was 9. *Id.* at ¶ 713.

<sup>56</sup> Lubanga and the UPC/FPLC’s actions regarding child soldiers were, tragically, hardly unique. Throughout the conflicts which ravaged the DRC beginning in 1996, “the use of child soldiers in armed groups was the rule, not the exception.” *Id.* at ¶ 62.

<sup>57</sup> *Id.* at ¶ 821.

<sup>58</sup> *Id.* at ¶ 835.

<sup>59</sup> *Id.* at ¶ 839.

<sup>60</sup> *Id.* at ¶ 878.



“kados”<sup>61</sup>, with “slightly fewer than 45 members.”<sup>62</sup>

The international criminal culpability threshold though is whether those functions constitute active participation in hostilities, the language from article 8 of the Rome Statute. Not surprisingly, the views of the parties in Lubanga on this issue diverged.

#### D. *Parties’ Views on Active Participation*

As the Lubanga Court noted, active participation is “not defined in the [Rome] Statute, the Rules or the Elements of Crimes.”<sup>63</sup> The prosecution and the legal representative for the victims adopted the meaning used by the pre-trial chamber in Lubanga that “active participation in hostilities means not only direct participation in hostilities but covers active participation in combat related activities such as scouting, spying, sabotage, and the use of children as decoys, couriers or at military check points.”<sup>64</sup>

The defense argued that active participation in hostilities equates to “acts of war, which by their nature or purpose are likely to cause actual harm to the personnel and equipment of the enemy armed forces.”<sup>65</sup> Not unreasonably, the court looked to the Special Court for Sierra Leone (SCSL), the first international tribunal to consider child soldier offenses.<sup>66</sup> In terms of child soldier offenses, the statute for the SCSL is identical to the Rome Statute.<sup>67</sup> In mapping the contours of active participation in hostilities, the SCSL noted that an armed force requires logistical support to maintain its operations. Any labor or support that gives effect to, or helps maintain, operations in a conflict constitutes active participation. Hence carrying loads for the fighting faction, finding and/or acquiring food, ammunition or equipment, acting as decoys,

---

<sup>61</sup> As one prosecution witness testified, “in the UPC and Ugandan armies, indeed in Africa generally, small children from about the age of 13 up to the age of 16 are called kados” *Id.* at ¶ 636.

<sup>62</sup> *Id.* at ¶ 871.

<sup>63</sup> *Id.* at ¶ 600.

<sup>64</sup> *Id.* at ¶ 591 (referring to confirmation of charges para 261). One difference between the views of the prosecutor and the victims representative was on whether active participation included girls recruited into the armed forces for sexual purposes. The victims representative argued it did, an argument the prosecutor did not make, and, as a result, one the court did not address. *Id.* at ¶ 598.

<sup>65</sup> *Id.* at ¶ 584.

<sup>66</sup> See Prosecutor v. Brima, Kamara and Kanu, Case No. SCSL-04-16-T, Judgment, (June 20, 2007), <http://www.unhcr.org/refworld/pdfid/467fba742.pdf> [hereinafter Brima Judgment].

<sup>67</sup> See UN Security Council, Statute of the Special Court for Sierra Leone art. 4(c) (Jan. 16, 2002), <http://www.unhcr.org/refworld/type,INTINSTRUMENT,,,3dda29f94,0.html> (listing “conscripting or enlisting children under the age of 15 into the armed forces or groups or using them to participate actively in hostilities” as a serious violation of international humanitarian law).

carrying messages, making trails or finding routes, manning checkpoints or acting as human shields are some examples of active participation as much as actual fighting and combat.<sup>68</sup>

The SCSL held that active participation is “not restricted to children directly involved in combat”<sup>69</sup> but “encompasses the use of children in functions other than as front line troops [] including support roles within military operations.”<sup>70</sup> But to constitute active participation, the support roles would need to put the child soldiers’ lives “directly at risk in combat.”<sup>71</sup>

The pretrial chamber in Lubanga elaborated, explaining that activities like serving as a bodyguard would need “to have a direct impact on the level of logistic resources and on the organization of operations required by the other party to the conflict”.<sup>72</sup> Conversely, “children who were engaged in activities ‘clearly unrelated to hostilities’... do not actively participate in hostilities.”<sup>73</sup> Both the pretrial and trial chambers in Lubanga rely on a draft version of the Rome Statute, which, in a footnote stated that the words “using” and “participate” have been adopted in order to cover both direct participation in combat and also active participation in military activities linked to combat such as scouting, spying, sabotage and the use of children as decoys, couriers or at military checkpoints. It would not cover activities clearly unrelated to the hostilities such as food deliveries to an airbase or the use of domestic staff in an officer’s married accommodation. However, use of children in a direct support function such as acting as bearers to take supplies to the front line, or activities at the front line itself, would be included within the terminology.<sup>74</sup>

Both chambers’ reliance is misplaced—in distinguishing between direct and active participation the footnote misstates the law. The *Lubanga* Court, in misapplying the misstatement, compounds the error. The result, while expanding the scope of Lubanga’s liability, decreased the scope of protection from attack international humanitarian law would otherwise afford to child

---

<sup>68</sup> Lubanga Judgment, *supra* note 2, at ¶ 624 (quoting Brima Judgment, *supra* note 68, at ¶ 737). The *Lubanga* Court’s analysis is largely based on, and follows, that of the SCSL. That the SCSL broadly defined active participation is also problematic and for the same reasons. But at least the SCSL issued its decisions before the ICRC issued the interpretative guidance on direct participation in hostilities. The ICC however issued the Lubanga decision over 3 years after the ICC published the interpretative guidance.

<sup>69</sup> Lubanga Judgment, *supra* note 2, at ¶ 624 (referring to Brima Judgment, *supra* note 68).

<sup>70</sup> Lubanga Judgment, *supra* note 2, at ¶ 625.

<sup>71</sup> Lubanga Judgment, *supra* note 2, at ¶ 626 (quoting Brima Judgment, *supra* note 68, at ¶ 736).

<sup>72</sup> Lubanga Judgment, *supra* note 2, at ¶ 624.

<sup>73</sup> *Id.* at ¶ 623 (quoting Prosecutor v. Thomas Lubanga Dyilo, Case No. ICC-01/04-01/06, Decision on the Confirmation of Charges (Jan. 29 2007) at ¶ 262).

<sup>74</sup> Lubanga Judgment, *supra* note 2, at ¶ 621.

soldiers like those in the UPC/FPLC. Those protections are qualified by how the term civilian is defined and whether their actions amount to direct participation in hostilities.

#### IV. CIVILIANS UNDER THE LAW OF ARMED CONFLICT

It is axiomatic that the law of armed conflict protects civilians from being the object of direct attack or “targeted.”<sup>75</sup> At first blush, child soldiers in the UPC/FPLC may not seem the “civilians” the law envisioned. But nowhere in the law of armed conflict is the term civilian positively defined. Despite the 1949 Fourth Geneva Convention’s focus on the protection of civilian persons in time of war, it doesn’t define who exactly is—and isn’t—a civilian.<sup>76</sup> Additional Protocol I does define the term civilian, but does so negatively in article 50. It states that “[a] civilian is any person who does not belong to one of the categories of persons referred to in Article 4 A(1); (2), (3) and (6) of the Third Geneva Convention and in Article 43 of [Additional Protocol].”<sup>77</sup> The definition concludes with “[i]n case of doubt whether a person is a civilian, that person shall be considered to be a civilian.”<sup>78</sup>

The references to Article 4 of the Third Geneva Convention, and to article 43 of AP I, are to persons who qualify for status as a prisoner of war. This includes:

- (1) Members of the armed forces of a Party to the conflict as well as members of militia or volunteer corps forming part of such armed forces;

---

<sup>75</sup> Additional Protocol I to the 1949 Geneva Conventions codifies the basic protections the law of armed conflict affords civilians from the application of force. These include that: “[t]he civilian population and individual civilians shall enjoy general protection against dangers arising from military operations....The civilian population as such, as well as individual civilians shall not be the object of attack. Acts of threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited.”

AP I, *supra* note 42, art. 51.

<sup>76</sup> Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 76 U.N.T.S. 287.

<sup>77</sup> AP I, *supra* note 42, art. 50. The International Committee of the Red Cross, in its commentary to article 50, further explains that this definition has the great advantage of being “ne varietur.” Its negative character is justified by the fact the concepts of the civilian population and the armed forces are only conceived in opposition to each other, that the later constitutes a category of persons which is now clearly defined in international law and determined in an indisputably manner by the laws and regulations of States. Therefore it was worth taking advantage of this possibility. It is clear that a negative definition of the civilian population implies that the meaning given to “armed forced” must be pointed out. ICRC Commentary to AP I, *supra* note 42, art. 50, sec. 1914.

<sup>78</sup> AP I, *supra* note 42, art. 50 (1). See Prosecutor v. Blaskic, Case No. IT-95-T, Judgment, ¶ 180 (Mar. 3 2000) (defining civilians as “persons who are not, or no longer, members of the armed forces.”).

- (2) Members of other militias and members of other volunteer corps, including those of organized resistance movements, belonging to a Party to the conflict and operating in or outside their own territory;
- (3) Members of regular armed forces who profess allegiance to a government of authority not recognized by the Detaining Power
- (6) Inhabitants of a non-occupied territory, who on the approach of the enemy spontaneously take up arms to resist the invading forces, without having time to form themselves into regular armed units.<sup>79</sup>

The UPC/FPLC does not fit in any of the categories.<sup>80</sup> Thus under the law of armed conflict's negative definition, its members, child or adult, are considered civilians. Having articulated, albeit indirectly, the definition of civilian, article 50 then qualifies the protections the law of armed conflict affords this class of individuals. "Civilians shall enjoy the protection afforded by this Section [of not being the target of the application of force] unless and for such time as they take a direct part in hostilities."<sup>81</sup>

The meaning and temporal limitations of the direct participation in hostilities qualification to the norm that civilians may not be targeted are among the most contentious areas of the law of armed conflict. But rather than add clarity to what does and does not constitute direct participation in hostilities, the *Lubunga* decision further muddled the field, further increasing the risk to child soldiers in the process.

#### A. *Active vs. Direct Participation*

Simply put, the *Lubunga* Court separates active from direct participation,

---

<sup>79</sup> Geneva Convention Relative to the Treatment of Prisoners of War, Art. 4, Aug. 12 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter Third Geneva Convention]. This obviously skips over two categories, (4) and (5). Four is "persons who accompany the armed forces without actually being members thereof, such a civilian members of military aircraft crews, war correspondents, supply contractors, members of labor units or of services responsible for the welfare of the armed forces...." Five is "members of crews, including masters, pilots and apprentices, of the merchant marine and the crews of civil aircraft of the Parties to the conflict, who do not benefit from by more favourable treatment under any other provisions of international law." *Id.* art. 4. Since these two categories are excepted from AP I's negative definition of civilian, these individuals are considered civilians. Finally, reference to art. 43 of AP I is to "the armed forces of a Party to a conflict....", which would qualify such individuals as prisoners of war and thus not as civilians. AP I, *supra* note 42, Art. 43.

<sup>80</sup> To qualify for prisoner of war status, and the attendant combatant immunity, the UPC/FPLC would also to fulfill the following conditions of Article 4(2): (a) that of being commanded by a person responsible for his subordinates; (b) that of having a fixed distinctive sign recognizable at a distance; (c) that of carrying arms openly; (d) that of conducting their operations in accordance with the laws and customs of war.

Third Geneva Convention, *supra* note 81, art. 4(2). At a minimum, the UPC/FPLC did not follow the laws of armed conflict and thus does not qualify.

<sup>81</sup> AP I, *supra* note 42, Art. 51(3).

but the law recognizes no such distinction. The International Committee of the Red Cross (ICRC), in its Interpretative Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law, stated that although the English texts of the Geneva Conventions and Additional Protocols use the words “active” and “direct”, respectively, the consistent use of the phrase “participer directement” in the equally authentic French texts demonstrate that the terms “direct” and “active” refer to the same quality and degree of individual participation in hostilities.<sup>82</sup>

Flowing from, or perhaps causing, the flawed attempt to disaggregate participation in hostilities, the *Lubanga* Court overstates the differences in the legal regimes applicable to international vs non-international conflict. Additional Protocol I to the Geneva Conventions, which governs international armed conflict, uses the term “participate directly”.<sup>83</sup> Additional Protocol II to the Geneva Conventions, which governs non-international armed conflicts, utilizes “to participate actively.”<sup>84</sup> The *Lubanga* Court claimed that [t]he use of the expression “to participate actively in hostilities”, as opposed to the expression “direct participation” (as found in Additional Protocol I to the Geneva Conventions) was clearly intended to import a wide interpretation to the activities and roles that are covered by the offence of using children under the age of 15 actively to participate in hostilities.<sup>85</sup>

In attempting to explain a distinction that doesn’t exist, the Court blithely noted that the participation in hostilities language of AP II “does not include the word “direct”.” That superficial analysis is literally true—but substantively false. The ICRC, in explaining the absence of the very distinction the *Lubanga* Court relied on, stated that “taking a direct part in hostilities is used synonymously in the Additional Protocols I and II, it should be interpreted in the same manner in international and non-international armed conflict.”<sup>86</sup>

Applying its flawed conception of direct vs active participation, the *Lubanga* Court concluded that those who participate actively in hostilities include a wide range of individuals, from those on the front line (who participate directly) through to the boys or girls who are involved in a myriad of roles that support the combatants. All of these activities, which cover either direct or indirect

---

<sup>82</sup> Nils Melzer, Int’l Comm. Of the Red Cross, *Interpretative Guidance on the Notion of Direct Participation in Hostilities Under International Law*, 90 INT’L REV. OF THE RED CROSS 991, 1013–14 (2009) (adopted by the assembly of the international committee of the Red Cross on February 26, 2009) [hereinafter ICRC Interpretive Guidelines].

<sup>83</sup> AP I, *supra* note 42, art. 43(2).

<sup>84</sup> AP II, *supra* note 44, art. (3)(c).

<sup>85</sup> *Lubanga* Judgment, *supra* note 2, ¶ 627.

<sup>86</sup> ICRC Interpretative Guidance, *supra* note 83, at 1014 (emphasis added). Moreover, that view is not just that of the ICRC but was the prevailing view of the legal experts who worked with the ICRC in developing the Interpretative Guidance.

participation, have an underlying common feature: the child concerned is, at the very least, a potential target.<sup>87</sup> Having failed to recognize that active and direct refer to the same level of participation, the court reaches the oxymoronic position of determining when indirect participation constitutes active participation. Essentially, the court is asking when indirect participation constitutes direct participation. It does not, it cannot.

The test the court develops for this inherently contradictory inquiry is that “[t]he decisive factor, therefore, in deciding if an “indirect” role is to be treated as active participation in hostilities is whether the support provided by the child to the combatants exposed him or her to real danger as a potential target.”<sup>88</sup> Not explaining the meaning of any of the substantive portions of this “decisive factor,”<sup>89</sup> the Court then expanded, without defining, the temporal nexus holding that In the judgment of the Chamber these combined factors—the child’s support and this level of consequential risk—mean that although absent from the immediate scene of the hostilities, the individual was nonetheless actively involved in them.”<sup>90</sup>

#### V. THE LUBANGA DECISION’S RISK TO CHILD SOLDIERS

The harm the *Lubanga* decision poses to child soldiers flows from attempting to distinguish active from direct participation in hostilities and then broadly defining what constitutes active participation. The result is an increased range of activities constituting direct participation. This renders child soldiers performing the actions targetable in the process.

Child soldiers who carry weapons and fight are directly participating and thus targetable. But as previously discussed, most child soldiers do not carry or use weapons, they provide a range of logistics or support functions. These functions constitute the almost limitless expansion of harm the Lubanga decision created for child soldiers.

In creating a space between direct and active participation, the court claimed that “[t]he travauxpréparatoires of the [Rome] Statute suggests that although direct participation is not necessary, a link with combat is nonetheless required.”<sup>91</sup> But as the ICRC observed, “[s]tandards such as “indirect causation of harm” are clearly too wide, as they would bring the entire war effort within the concept of direct participation in hostilities and, thus, would deprive large

---

<sup>87</sup> Lubanga Judgment, *supra* note 2, ¶ 628.

<sup>88</sup> *Id.* ¶ 628.

<sup>89</sup> For example, the words “expose”, “potential” and “target” all warrant definition. And the use of “real danger” is particularly unhelpful. As opposed to what kind of danger?

<sup>90</sup> *Id.*

<sup>91</sup> *Id.* ¶ 621.

parts of the civilian population of their protection against direct attack.”<sup>92</sup> The ICC’s test for indirect active participation, whether the child soldier’s activities exposed him or her to “real danger,” is equally problematic. Under this test, unarmed child soldier activities related to hostilities, which have a direct impact on logistic resources constitute active participation. Finding, carrying, and providing food for example, could all qualify.

By way of comparison, the ICRC concluded that there are three constitutive elements to direct participation in hostilities:

- (1) The harm likely to result from the act must attain a certain threshold;
- (2) There must be a direct causal link between the act and the harm likely to result;
- (3) The act must be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another.<sup>93</sup>

These elements exclude conduct (and thus preclude targeting) which the *Lubanga* Court would include. Returning to logistics resources, the ICRC recognized that providing food to the armed forces is “indispensable.”<sup>94</sup> But providing food is not directly causal to the infliction of harm and as a result does not constitute DPH.<sup>95</sup>

Even the *Lubanga* Court’s limits on active participation are problematic. The court mentions that “food deliveries to an airbase or the use of domestic staff in married officer’s quarters” do not constitute active participation.<sup>96</sup> The qualifications on the limitations are troubling. It is not that food deliveries per se do not qualify, but that food deliveries to an airbase do not.<sup>97</sup> The implication is that food delivery to the front line of hostilities might, as the unarmed child doing so would exposed to risk. Similarly, the court could have but did not say domestic work per se does not amount to active participation. Similar to food delivery, the court qualified the limitation, here to married officer’s quarters. One can envision child soldiers performing domestic work closer to the scene of hostilities than married officer’s spouses and quarters would be located. Again, under the *Lubanga* decision, where the domestic work exposed the child to “real danger”, the work presumably qualifies as

<sup>92</sup> ICRC Interpretative Guidance, *supra* note 83.

<sup>93</sup> *Id.* The defense in *Lubanga* argued for the court to use the three factors and a narrow definition of participation. *Lubanga* Judgment, *supra* note 2, ¶ 585.

<sup>94</sup> ICRC Interpretative Guidance, *supra* note 83.

<sup>95</sup> *Id.*

<sup>96</sup> *Lubanga* Judgment, *supra* note 2, ¶ 623.

<sup>97</sup> The airbase reference is itself odd as the organized armed groups, which employ child soldiers, do not possess air power. An example with a never occurring predicate is not particularly illuminating.

active participation. This expansive view of participation may prove more retributive than protective of child soldiers.

To maintain balance between the mutual aspects of participation, the court should limit active participation to those activities that constitute DPH under the ICRC's interpretative guidance. This would also eliminate what is an otherwise glaring and problematic discrepancy between how the ICRC and the ICC define participation in hostilities. To ensure that the use of child soldiers in all its forms is criminalized, the Assembly of States Parties to the Rome Statute could modify the statute to include indirect participation.<sup>98</sup>

Any retributive legacy from the Lubanga case probably will not directly arise in the child soldier context. Rather a defendant before the ICC or other international tribunal who is charged with wrongful killing may utilize the *Lubanga* Court's analysis in a way neither the prosecutor nor the court probably ever envisioned and certainly never intended. The defendant will argue that the victims' logistic or support roles constitute direct participation in hostilities and thus targeting them was permissible under the law of armed conflict.<sup>99</sup> While such an argument may well fall short, international criminal justice deserved to be able to rely on and not have to distinguish if not disavow the ICC's first case.

## VI. CONCLUSION

In *Lubanga*, the prosecutor argued for a broader definition of participation in hostilities "in order to afford wider protection to child soldiers."<sup>100</sup> The attendant methodological compromises and contradictions increased one defendant's liability, but eroded that very protection in the process.



---

<sup>98</sup> The statute could incorporate the *Lubanga* court's point about risk to the child soldier in differing penalties for direct and indirect participation in hostilities.

<sup>99</sup> Such a defendant could argue that the victims' deaths per se prove the other component of the test the *Lubanga* Court developed—that they were in real danger.

<sup>100</sup> *Lubanga* Judgment, *supra* note 2, ¶ 578.



STUDENT NOTE

Separate But Equal Accountability: The Case of Omar Khadr

Grantland Lyons\*

ABSTRACT

*This Note addresses the question of whether to hold child combatants or their commanders accountable for war crimes, and if so, how and to what extent. The author ultimately concludes that child combatants and their commanders should be held equally accountable for their actions, but by measures that appropriately balance individual and public interests in rehabilitation, reintegration, and deterrence.*

*The Note focuses on Omar Khadr, a former child combatant, while using other cases as a reference point for current international legal norms. The author analyzes Khadr’s combatant status review, subsequent legal proceedings, detention, and sentence in light of various legal and policy considerations. The author maintains that despite the objectionable means used to obtain Khadr’s conviction, it was at least proportionate to the war crimes that he allegedly committed. However, the author also suggests which measures would have been more appropriate under the circumstances and recommends measures that could be taken with respect to similar cases in the future.*

Table of Contents

I. INTRODUCTION.....	126
II. BACKGROUND.....	127
A. The “War on Terror”.....	127
B. Guantánamo Military Commissions.....	127
C. Omar Khadr.....	128
III. STATUS REVIEW.....	129
A. Overview.....	129
B. Khadr as Child Soldier.....	130
i. Legal Justifications.....	130
a. International Instruments.....	130

\* University of Miami School of Law, Class of 2013. Special thanks to Professor Edgardo Rotman for supervising this writing project.

<i>b. Lack of Precedent</i> .....	132
<i>ii. Policy Justifications</i> .....	134
<i>a. Developmental Vulnerabilities</i> .....	134
<i>b. Rehabilitation Capacity</i> .....	136
IV. CONSEQUENCES.....	136
A. <i>Denial of Special Protections</i> .....	136
i. Presumption of Victimization.....	137
ii. Rehabilitation and Reintegration.....	139
iii. Immunity from Continuing Prosecution.....	139
B. <i>Denial of Substantive Rights and Procedural Safeguards</i> .....	140
i. Habeas Petitions.....	140
ii. Assistance of Counsel.....	141
iii. Evidentiary Issues.....	142
<i>a. Reliability</i> .....	142
<i>b. Accessibility</i> .....	142
C. <i>Unlawful Detention</i> .....	143
i. Duration.....	144
ii. Conditions.....	144
<i>a. Minimum Standards</i> .....	144
<i>b. Child-Specific Standards</i> .....	145
V. PLEA AGREEMENT & SENTENCE.....	145
A. <i>Overview</i> .....	145
B. <i>Assessment</i> .....	146
i. The Plea Agreement.....	146
ii. The Sentence.....	146
<i>a. American Perspective</i> .....	147
<i>b. Comparative Perspective</i> .....	147
VI. CONCLUSIONS & RECOMMENDATIONS.....	148

## I. INTRODUCTION

This past year marked a watershed for international juvenile justice. Omar Khadr, a Canadian national who was captured as a minor by US forces in Afghanistan and detained for over eight years in Guantánamo, was finally repatriated to his homeland after accepting a plea agreement.<sup>1</sup> Meanwhile in The Hague, Thomas Lubanga Dyilo became the first defendant convicted by the International Criminal Court (“ICC”) for enlisting and using child soldiers under the age of fifteen.<sup>2</sup> These cases highlight some of the underlying issues that

<sup>1</sup> *Omar Khadr returns to Canada*, CBC NEWS CANADA (Sept. 29, 2012) [hereinafter CBC Report], <http://www.cbc.ca/news/canada/story/2012/09/29/omar-khadr-repatriation.html>.

<sup>2</sup> David Smith, *Thomas Lubanga sentenced to 14 years for Congo War Crimes*, THE GUARDIAN

still pervade the effective administration of juvenile justice abroad. Specifically, this article addresses the question of whether to hold child combatants or their commanders accountable for war crimes, and if so, how and to what extent. The article focuses on Khadr's case while using Lubanga's case and others as a reference point for current international legal norms.

Part II provides background information on the "War on Terror," Guantánamo Bay, and Khadr's case. Part III analyzes Khadr's combatant status review in light of legal and policy considerations and asserts that he should have been classified as a child soldier. Part IV discusses the consequences of Khadr's status review, including the inadequacy of his subsequent legal proceedings and detention, relative to the special protections that he should have received as a juvenile. Part V analyzes Khadr's plea agreement and sentence, and maintains that despite the objectionable means used to obtain them, the end result was at least proportionate to the war crimes he allegedly committed. Part VI concludes that child combatants and their commanders should be held equally accountable for their actions, but in different ways. For this reason, I explain which accountability measures would have been more appropriate under the circumstances and recommend measures that could be taken with respect to similar cases in the future.

## II. BACKGROUND

### A. *The "War on Terror"*

In response to the terrorist attacks of September 11, 2001, as well as the "continuing and immediate threat of further attacks on the United States," President Bush declared a state of emergency.<sup>3</sup> Congress also passed a joint resolution, authorizing the President to use "all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States."<sup>4</sup> This "War on Terror" has continued to the present day.

### B. *Guantánamo Military Commissions*

In November 2001, President Bush authorized the use of military

---

(July 10, 2012), available at <http://www.guardian.co.uk/law/2012/jul/10/icc-sentences-thomas-lubanga-14-years>.

<sup>3</sup> Proclamation No. 7463, 66 Fed. Reg. 48199 (Sept. 14, 2001), available at <http://www.fas.org/irp/news/2001/09/fr091801.html>.

<sup>4</sup> S.J. Res. 23, 107th Cong. (2001), available at <http://www.law.cornell.edu/background/warpower/sj23.pdf>.

commissions to try suspected terrorists for crimes.<sup>5</sup> US facilities in Guantánamo Bay, Cuba opened in 2002 to detain “unlawful enemy combatants” captured in the “War on Terror” and to further investigate threats of terrorism.<sup>6</sup> Some practices in Guantánamo have been heavily criticized.<sup>7</sup> The aim of this Note, however, is to examine one case in more detail, while attempting to reserve any judgment on U.S. foreign policy or general practices in Guantánamo.

In response to criticism, and upon taking office in 2009, President Obama halted the proceedings to review their continued use. The President soon issued an executive order requiring that Guantánamo be closed less than a year from that date.<sup>8</sup> The deadline for closing the detention facility at Guantánamo passed, but the Obama administration reportedly determined that about 50 of the suspects held there would continue to be detained without trial, about 40 detainees would be prosecuted in military commissions or federal court, and the remaining 110 detainees would be released to suitable countries that have agreed to accept them.<sup>9</sup>

### C. Omar Khadr

The American Civil Liberties Union recently estimated that since Guantánamo's opening, the prison has detained 21 alleged juvenile offenders.<sup>10</sup> One such offender, Omar Khadr, was only fifteen years old when he was captured by U.S. forces in Afghanistan and taken into U.S. custody.<sup>11</sup> Khadr was transferred to Guantánamo in 2003, where he was charged under

---

<sup>5</sup> Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terrorism, 66 Fed. Reg. 57833 (Nov. 16, 2001), § 1(a), *available at* <http://www.law.cornell.edu/background/warpower/fr1665.pdf>, *see also* Department of Defense, *President Determines Enemy Combatants Subject to His Military Order* (July 3, 2003), *available at* <http://www.defense.gov/releases/release.aspx?releaseid=5511>.

<sup>6</sup> Meagan McElroy, *Features: Guantánamo Bay*, JURIST (updated Apr. 20, 2013), *available at* <http://jurist.org/feature/2012/01/guantanamo.php>.

<sup>7</sup> *See, e.g.*, Amnesty International, *Speech by Irene Khan at Foreign Press Association* (May 25, 2005) (regarding allegations of abuse and torture at Guantánamo), *available at* <http://web.archive.org/web/20060220210041/http://web.amnesty.org/library/Index/ENGPOL100142005>.

<sup>8</sup> Executive Order 13492, Review and Disposition of Individuals Detained at the Guantánamo Bay Naval Base and Closure of Detention Facilities, 74 Fed. Reg. 4897 (Jan. 22, 2009), *available at* <http://www.gpo.gov/fdsys/pkg/FR-2009-01-27/pdf/E9-1893.pdf>.

<sup>9</sup> Charlie Savage, *Detainees Will Still Be Held, but Not Tried, Official Says*, N.Y. TIMES (Jan. 22, 2010), *available at* <http://www.nytimes.com/2010/01/22/us/22gitmo.html>.

<sup>10</sup> American Civil Liberties Union, *Guantánamo by the Numbers* (updated Dec. 27, 2012), *available at* <http://www.aclu.org/national-security/Guantanamo-numbers>.

<sup>11</sup> *United States v. Khadr*, Charges, ¶¶ 12, 20, *available at* <http://www.defense.gov/news/nov2005/d20051104khadr.pdf>.

the U.S. military commissions system with conspiracy, murder by an unprivileged belligerent, attempted murder by an unprivileged belligerent, and aiding the enemy.<sup>12</sup>

The U.S. government alleged that when Khadr was only 10 years old, he and his father maintained close, continuous contact with Usama bin Laden and other senior members of al Qaida, a non-State armed terrorist organization with deeply-held Muslim beliefs.<sup>13</sup> They visited al Qaida training camps and guesthouses,<sup>14</sup> and even made yearly trips to Jalalabad to visit bin Laden.<sup>15</sup> For these reasons, al Qaida operatives likely recruited and indoctrinated Omar when he was still a minor. His family continued to move frequently throughout Afghanistan.<sup>16</sup> In the summer of 2002, Omar received personalized al Qaida weapons and landmines training.<sup>17</sup> After completing his training, Khadr conducted surveillance and reconnaissance against the U.S. military. For example, he went to an airport near Khost, Afghanistan, and watched U.S. convoys in support of future attacks.<sup>18</sup> Shortly thereafter, he planted explosive devices in the ground where U.S. forces were known to travel.<sup>19</sup> While engaged in a firefight with U.S. forces, Khadr threw a grenade, killing Sergeant First Class Christopher Speer.<sup>20</sup>

### III. STATUS REVIEW

#### A. Overview

In 2004, before any formal charges were filed, Khadr's combatant status was reviewed by the Combatant Status Review Tribunal ("CSRT").<sup>21</sup> The CSRT concluded, by a preponderance of the evidence, that: Khadr was mentally and physically capable of participating in the proceedings; he understood the proceedings but chose not to participate; and that he was properly classified as an enemy combatant.<sup>22</sup> The CSRT defined an enemy combatant as "an individual who was part of or supporting the Taliban or al Qaida forces, or associated forces that are engaged in hostilities against the United States or its

---

<sup>12</sup> *Id.* at ¶¶ 21ff.

<sup>13</sup> *Id.* at ¶ 16.

<sup>14</sup> *Id.*

<sup>15</sup> *Id.*

<sup>16</sup> *Id.* at ¶ 17.

<sup>17</sup> *Id.* at ¶¶ 22(a), 22(c).

<sup>18</sup> *Id.* at ¶ 22(b).

<sup>19</sup> *Id.* at ¶ 22(d).

<sup>20</sup> *Id.* at ¶ 22(e).

<sup>21</sup> Review of Combatant Status Review Tribunal No. 5, *Khadr v. Bush*, 587 F. Supp. 2d 225, available at [http://humanrights.ucdavis.edu/projects/the-guantanamo-testimonials-project/testimonies/testimonies-of-the-defense-department/csrts/csrt\\_isn\\_766.pdf](http://humanrights.ucdavis.edu/projects/the-guantanamo-testimonials-project/testimonies/testimonies-of-the-defense-department/csrts/csrt_isn_766.pdf).

<sup>22</sup> *Id.* at 10.

coalition partners. This includes any person who committed a belligerent act or has directly supported hostilities in aid of enemy armed forces.”<sup>23</sup> Even after the military commissions system was invalidated by the U.S. Supreme Court,<sup>24</sup> the CSRT’s definition remained consistent with the definitions provided in the Military Commissions Act of 2006<sup>25</sup> (“2006 MCA”) and its 2009 amendment<sup>26</sup> (“MCA Amendment”) (together, “MCA”). Based on the MCA’s distinction between “lawful” and “unlawful” enemy combatants,<sup>27</sup> Khadr was charged as the latter—without regard to his age—and remained in custody at Guantánamo.

### B. *Khadr as Child Soldier*

Because of his age and circumstances surrounding the alleged offenses, Khadr should have been classified as a child soldier. The UN Convention on the Rights of the Child (“CRC”) defines a child as “every human being below the age of eighteen years.”<sup>28</sup> The United Nations Children’s Fund further defines a “child soldier” as “any child . . . who is part of any kind of regular or irregular armed force or armed group in any capacity, including, but not limited to: cooks, porters, messengers, and anyone accompanying such groups other than family members. It includes girls and boys recruited for forced sexual purposes and/or forced marriage. The definition, therefore, does not only refer to a child who is carrying, or has carried, weapons.”<sup>29</sup> This is an enhanced status that could have justified Khadr’s release, and at the very least, would have afforded him greater protections under international law (see Part IV, *infra*). Various legal and policy reasons support such a classification.

#### i. Legal Justifications

##### a. *International Instruments*

The overwhelming accumulation of international treaty law and State practice confirms the unique vulnerability of children, especially child soldiers. The 1924 Geneva Declaration laid the foundation for modern children’s rights,

<sup>23</sup> *Id.* at 13.

<sup>24</sup> See *Hamdan v. Rumsfeld*, 548 U.S. 557, 634 (2006) [hereinafter *Hamdan*].

<sup>25</sup> See 10 USC § 948(a), Military Commissions Act [hereinafter 2006 MCA], available at <http://uscode.house.gov/download/pls/10C47A.txt>.

<sup>26</sup> See *id.* (as amended) [hereinafter MCA Amendment].

<sup>27</sup> See 2006 MCA and MCA Amendment, *supra* notes 25 and 26 [hereinafter “MCA”].

<sup>28</sup> Convention on the Rights of the Child, G.A. Res. 44/25, U.N. Doc. A/44/49 (Nov. 20, 1989) [hereinafter CRC], available at <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx>.

<sup>29</sup> UNICEF Factsheet, available at <http://www.unicef.org/emerg/files/childsoldiers.pdf>; Factsheet based on the Cape Town Principles (1997), available at [http://www.unicef.org/emerg/files/Cape\\_Town\\_Principles\(1\).pdf](http://www.unicef.org/emerg/files/Cape_Town_Principles(1).pdf).

stating, *inter alia*, that they “must be protected against every form of exploitation.”<sup>30</sup> The 1959 Declaration of the Rights of the Child expanded on that principle, adding that the child, “by reason of his physical and mental immaturity, needs special safeguards and care, including appropriate legal protection.”<sup>31</sup> The CRC, adopted in 1989, emphasizes the principles of non-discrimination, children’s participation, and the best interests of the child.<sup>32</sup> The Millennium Declaration considers children to be among the “most vulnerable.”<sup>33</sup> The Declaration accordingly calls upon States to “spare no effort [to give them] . . . every assistance and protection,” and to that end, ratify and implement the CRC with its protocols.<sup>34</sup>

International humanitarian law extends children’s protection during and after wartime. For example, many provisions in the Geneva Conventions (1949) and its additional protocols are recognized as customary international law and frequently distinguish between different age groups. Within Geneva Convention III, Article 16 requires that age be taken into account in assigning positions, while Article 49 requires age differentiation among laborers.<sup>35</sup> Within Geneva Convention IV, Article 24 outlines specific provisions for children under 15 years old, Article 50 imposes child-specific obligations upon occupying powers, Article 51 excludes children under 18 years old from any circumstances that may subject them to an occupying power, and Article 68 excludes children from the death penalty if they were under 18 years old when the alleged offense was committed.<sup>36</sup> Article 77(1) of Protocol I further provides that children “shall be the object of special respect” and that Parties to the conflict “shall provide them with the care and aid they require.”<sup>37</sup> Article 4(3) of Protocol II also provides that children are entitled, by virtue of

---

<sup>30</sup> Geneva Declaration on the Rights of the Child (Sept. 26, 1924), *available at* <http://www.un-documents.net/gdrc1924.htm>.

<sup>31</sup> Declaration of the Rights of the Child, G.A. Res. 1386 (XIV), U.N. Doc. A/4354 (Dec. 10, 1959), *available at* [http://www.unicef.org/lac/spbarbados/Legal/global/General/declaration\\_child1959.pdf](http://www.unicef.org/lac/spbarbados/Legal/global/General/declaration_child1959.pdf).

<sup>32</sup> *See, e.g., id.* at Preamble, art. 1.

<sup>33</sup> U.N. Millennium Declaration, G.A. Res. 55/2, ¶ 2 (Sept. 18, 2000), *available at* <http://www.un.org/millennium/declaration/ares552e.htm>.

<sup>34</sup> *Id.* at ¶ 26.

<sup>35</sup> Geneva Convention III Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 75 U.N.T.S. 135, *available at* <http://www.icrc.org/ihl.nsf/FULL/375>.

<sup>36</sup> Geneva Convention IV Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 75 U.N.T.S. 287, *available at* <http://www.icrc.org/ihl.nsf/full/380>.

<sup>37</sup> Additional Protocol 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 [hereinafter Protocol I], *available at* <http://www.icrc.org/ihl.nsf/full/470?opendocument>.

their age, to special protections.<sup>38</sup>

Other legal instruments highlight children's vulnerability in such circumstances. The CRC, for example, contains several provisions relating to armed conflict.<sup>39</sup> States Parties are obliged "to promote physical and psychological recovery and social reintegration" in "an environment which fosters the health, self-respect and dignity of the child."<sup>40</sup> The 2005 World Summit Outcome, recalling the Millennium Declaration principles, calls upon States to take measures preventing the recruitment and use of children in armed conflict, to criminalize such practices, and to ensure that children in armed conflicts receive "timely and effective humanitarian assistance, including education, for their rehabilitation and reintegration into society."<sup>41</sup>

### *b. Lack of Precedent*

Although prosecutions of child soldiers are not expressly prohibited under international law, no international criminal tribunal has ever prosecuted a former child soldier for alleged war crimes. Some tribunals that have limited jurisdiction over minors (discussed in more detail below) are rare and have never exercised any such jurisdiction.

When the Rome Statute of the ICC was drafted, countries made varying proposals for a universally acceptable age of criminal responsibility. According to a commentary of the Rome Statute's drafting history, no one under 18 years old was ever charged with any crime by the Nuremberg courts.<sup>42</sup> For that reason, States involved in the statute's drafting agreed that under international law criminal responsibility begins at 18 years old.<sup>43</sup> Consequently, the Rome Statute now reads that "[t]he Court shall have no jurisdiction over any person who was under the age of 18 at the time of the alleged commission of a crime."<sup>44</sup> In exercising that jurisdiction, Luis Moreno Ocampo, an ICC prosecutor, charged Thomas Lubanga Dyilo with the war crimes of enlisting

---

<sup>38</sup> Additional Protocol 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 Protocol II], *available at* <http://www.icrc.org/ihl.nsf/full/475?opendocument>.

<sup>39</sup> CRC, *supra* note 29, at art. 38-39.

<sup>40</sup> *Id.* at art. 39.

<sup>41</sup> 2005 World Summit Outcome, U.N. Doc. A/RES/60/1, ¶¶ 117-118 (Oct. 24, 2005), *available at* <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/487/60/PDF/N0548760.pdf>.

<sup>42</sup> OTTO TRIFFTERER, ed., COMMENTARY ON THE ROME STATUTE OF THE INTERNATIONAL CRIMINAL COURT: OBSERVERS' NOTES, ARTICLE BY ARTICLE 494 (1999).

<sup>43</sup> *Id.*

<sup>44</sup> Rome Statute of the International Criminal Court art. 26, July 17, 1998, U.N. Doc. A/CONF.183/9, 2187 U.N.T.S. 90 [hereinafter Rome Statute], *available at* [http://untreaty.un.org/cod/icc/statute/english/rome\\_statute\(e\).pdf](http://untreaty.un.org/cod/icc/statute/english/rome_statute(e).pdf).



and using children under the age of fifteen to participate actively in hostilities.<sup>45</sup> The court convicted Lubanga on the grounds that his leadership activities subjected children to “real danger” as potential targets of violence.<sup>46</sup>

The UN Security Council established the Special Court for Sierra Leone (“SCSL”) to prosecute “persons who bear the greatest responsibility” for crimes committed during its civil war, particularly those who led the recruitment and exploitation of child soldiers.<sup>47</sup> The SCSL’s statute provides the court jurisdiction over children between 15-18 years old but requires that they be treated “with dignity and a sense of worth, taking into account his or her young age and the desirability of promoting his or her rehabilitation, reintegration into and assumption of a constructive role in society.”<sup>48</sup> The court also has the power to order juvenile-appropriate measures, including care guidance, supervision, community service, counseling, foster care, and correctional and educational programs.<sup>49</sup> Nonetheless, the Security Council believed that the Sierra Leone Truth and Reconciliation Commission could probably serve this purpose better than the courts.<sup>50</sup>

Other *ad hoc* tribunals have taken similar deliberate measures. Neither statute for the International Criminal Tribunal for the Former Yugoslavia,<sup>51</sup> nor Rwanda,<sup>52</sup> contains any provisions regarding the minimum age of criminal responsibility. However, should the courts have sought to exercise jurisdiction

---

<sup>45</sup> *Prosecutor v. Lubanga Dyilo*, No. ICC-01/04-01/06, Warrant of Arrest (Jan. 12, 2001), available at <http://www.icc-cpi.int/iccdocs/doc/doc191959.PDF>.

<sup>46</sup> *Prosecutor v. Lubanga Dyilo*, No. ICC-01/04-01/06, Judgment, ¶ 628 (Mar. 14, 2012) [hereinafter *Lubanga*], available at <http://www.icc-cpi.int/iccdocs/doc/doc1379838.pdf>.

<sup>47</sup> U.N. Secretary-General, Letter dated Jan. 12, 2001 from the Secretary-General addressed to the President of the General Assembly, U.N. Doc. S/2001/40, at 1, available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/211/71/PDF/N0121171.pdf>.

<sup>48</sup> Statute of the Special Court for Sierra Leone art. 7(1), U.N. Doc. S/RES/1315 (Aug. 14, 2000) [hereinafter *SCSL Statute*], available at <http://www.sc-sl.org/LinkClick.aspx?fileticket=uClnD1MJEW=&>.

<sup>49</sup> *Id.* at art. 7(2).

<sup>50</sup> U.N. Security Council President, Letter dated Dec. 20, 2000 from the President of the Security Council addressed to the Secretary-General, U.N. Doc. S/2000/1234, at 1, available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N00/812/77/PDF/N0081277.pdf>.

<sup>51</sup> Statute of the International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1991, Annex, U.N. Doc. S/25704 (May 3, 1993), available at [http://www.icty.org/x/file/Legal Library/Statute/statute\\_re808\\_1993\\_en.pdf](http://www.icty.org/x/file/Legal%20Library/Statute/statute_re808_1993_en.pdf).

<sup>52</sup> Statute of the International Criminal Tribunal for the Prosecution of Persons Responsible for Genocide and Other Serious Violations of International Humanitarian Law Committed in the Territory of Rwanda and Rwandan Citizens Responsible for Genocide and Other Such Violations Committed in the Territory of Neighboring States, between Jan. 1, 1994 and Dec. 31, 1994, Annex, U.N. Doc. S/RES/955 (1994), available at [http://www.un.org/ga/search/view\\_doc.asp?symbol=S/RES/955\(1994\)](http://www.un.org/ga/search/view_doc.asp?symbol=S/RES/955(1994)).

over a minor, he or she could raise age as an affirmative defense.<sup>53</sup> The Extraordinary Chambers in the Courts of Cambodia limit their jurisdiction to “those who were most responsible” for war crimes during the Khmer Rouge period.<sup>54</sup> Should a court decide that a minor was among those most responsible, however, the purpose of any prosecution would still be rehabilitative rather than retributive.<sup>55</sup> The Special Panels for Serious Crimes in East Timor may prosecute minors between 12-16 years old, but “only in accordance with such rules as may be established in subsequent [United Nations Transitional Administration in East Timor] regulations on juvenile justice,” which must accord with the CRC and “shall consider his or her juvenile condition in every decision made in the case.”<sup>56</sup> The CRC, in turn, provides that measures relating to children in armed conflict should be intended to promote physical and psychological recovery and social reintegration.<sup>57</sup>

ii. Policy Justifications

a. *Developmental Vulnerabilities*

Recent social science research confirms that juveniles are much less capable of controlling their behavior, and therefore are less culpable than adults.<sup>58</sup> Generally speaking, juveniles are more willing to take risks than adults and more likely to believe that they can avoid negative consequences of taking

---

<sup>53</sup> See U.N. Secretary-General, *Rep. of Secretary General Pursuant to Paragraph 2 of S.C. Res. 808*, ¶ 58, U.N. Doc. S/2570 (1993) (stating that the tribunals must decide if age or mental incapacity may relieve a person of individual criminal responsibility), available at [http://www.icty.org/x/file/Legal Library/Statute/statute\\_re808\\_1993\\_en.pdf](http://www.icty.org/x/file/Legal%20Library/Statute/statute_re808_1993_en.pdf).

<sup>54</sup> Law on the Extraordinary Chambers in the Courts of Cambodia for the Prosecution of Crimes Committed During the Period of Democratic Kampuchea art. 1, NS/RKM/1004/006, available at [http://www.eccc.gov.kh/sites/default/files/legal-documents/KR\\_Law\\_as\\_amended\\_27\\_Oct\\_2004\\_Eng.pdf](http://www.eccc.gov.kh/sites/default/files/legal-documents/KR_Law_as_amended_27_Oct_2004_Eng.pdf).

<sup>55</sup> See *id.* at art. 33 (providing that courts shall exercise jurisdiction in accordance with international standards . . . as set out in the 1966 International Covenant on Civil and Political Rights [hereinafter ICCPR]), see also ICCPR art. 14(4), G.A. Res. 2200A (XXI), U.N. Doc. A/6316, 999 U.N.T.S. 171 (1966) (stating that criminal process over minors must “take account of their age and the desirability of promoting their rehabilitation”).

<sup>56</sup> U.N. Transitional Authority in East Timor on Transitional Rules of Criminal Procedure art. 45, Reg. 2000/30, available at <http://www.eastimorlawjournal.org/UNTAETLaw/Regulations/Reg2000-30.pdf>.

<sup>57</sup> CRC, *supra* note 29, at art. 39.

<sup>58</sup> *Roper v. Simmons*, 543 U.S. 551, 567 (2005) [hereinafter Simmons] (citing Jeffrey Arnett, *Reckless Behavior in Adolescence: A Developmental Perspective*, 12 DEV. REV. 339 (1992); Laurence Steinberg & Elizabeth Scott, *Less Guilty by Reason of Adolescence: Developmental Immaturity, Diminished Responsibility, and the Juvenile Death Penalty*, 58 AM. PSYCHOLOGIST 1009, 1014 (2003); ERIK ERIKSON, *IDENTITY: YOUTH AND CRISIS* (1968)).

such risks.<sup>59</sup> They may be unaware of all the risks involved or fail to properly calculate the risks involved. Whether due to their young age, uncertainty about the future, reduced stake in life, or other relevant factors, they also tend to focus more on short-term than long-term consequences,<sup>60</sup> and often fail to appreciate the real costs of their decisions and behavior.<sup>61</sup> Juveniles also tend to resist social controls and deterrence measures.<sup>62</sup>

At the same time, however, they are more easily influenced by their peers and by how they perceive themselves.<sup>63</sup> Peer pressure can play a major role in the commission of crimes, as most delinquent behavior occurs in groups.<sup>64</sup> Human rights groups similarly acknowledge that children are vulnerable to military recruitment because they are “easily manipulated and can be drawn into violence that they are too young to resist or understand.”<sup>65</sup> As a whole, juveniles have less control over their environment, which plays an important role in their development.<sup>66</sup>

These generalities apply to Khadr’s case because senior operatives of al Qaida, a powerful and influential organization, recruited and trained him from a young age. His father maintained close contact with those operatives, and may have encouraged or even compelled his young son to join the organization. Khadr’s family was always on the move during an unstable time in Afghanistan’s history, so he probably lacked any real control over his environment. Khadr attended numerous events and summer camps, and probably associated with other boys his age, so these people exerted a considerable amount of influence on him over time. Thus Khadr seems to have joined and remained in the organization for social, political, and perhaps to

---

<sup>59</sup> Elizabeth Cauffman & Laurence Steinberg, *(Im)maturity of Judgment in Adolescence: Why Adolescents May Be Less Culpable Than Adults*, 18 BEHAV. SCI. & L. 741, 752 (2000), available at [http://www.oja.state.ok.us/SAG Website/MacFound/\(Im\)maturity\\_of\\_Judgment\\_Article.pdf](http://www.oja.state.ok.us/SAG Website/MacFound/(Im)maturity_of_Judgment_Article.pdf).

<sup>60</sup> Elizabeth Scott, *Evaluating Adolescent Decision Making in Legal Contexts*, 19 L. & HUM. BEHAV. 221, 231 (1995) [hereinafter Scott].

<sup>61</sup> Christopher Slobogin, *A Prevention Model of Juvenile Justice: The Promise of Kansas v. Hendricks for Children*, 1999 WIS. L. REV. 185, 199 (1999); Thomas Grisso & Laurence Steinberg, *Juveniles’ Competence to Stand Trial: A Comparison of Adolescents and Adults’ Capacities as Trial Defendants*, 27 L. & HUM. BEHAV. 333, 353-56 (2003), available at [http://stopyouthviolence.ucr.edu/pubs\\_by\\_topic/5.Juveniles’ competence to stand trial.pdf](http://stopyouthviolence.ucr.edu/pubs_by_topic/5.Juveniles%20competence%20to%20stand%20trial.pdf).

<sup>62</sup> Carl Keane, *Deterrence and Amplification of Juvenile Delinquency by Police Contact: The Importance of Gender and Risk-Orientedness*, 29 BRIT. J. CRIMINOLOGY 336, 338 (1989).

<sup>63</sup> Thomas Berndt, *Developmental Changes in Conformity to Peers and Parents*, 15 DEV. PSYCH. 608, 615 (1979); Scott, *supra* note 61, at 230.

<sup>64</sup> Franklin Zimring, *Kids, Groups and Crime: Some Implications of a Well-Known Secret*, 72 J. CRIM. L. & CRIMINOLOGY 867, 867 (1981).

<sup>65</sup> See, e.g., Human Rights Watch Factsheet, *Facts about Child Soldiers*, available at <http://www.hrw.org/news/2008/12/03/facts-about-child-soldiers>.

<sup>66</sup> Simmons, *supra* note 59, at 569.

some degree, economic stability.

*b. Rehabilitation Capacity*

Recent social research also suggests that children generally have a greater capacity to rehabilitate than adults.<sup>67</sup> In *Roper v. Simmons*, the U.S. Supreme Court recognized that because juveniles “still struggle to define their identity[,] . . . the signature qualities of youth are transient.”<sup>68</sup> Therefore, in the Court’s view, “it would be misguided to equate the failings of a minor with those of an adult, for a greater possibility exists that a minor’s character deficiencies will be reformed. . . . [T]he impetuosity and recklessness that may dominate in younger years can subside.”<sup>69</sup> Given Khadr’s capacity to rehabilitate, it was improper for the military commission to classify Khadr as an enemy combatant rather than a child soldier.

IV. CONSEQUENCES

*A. Denial of Special Protections*

International law requires that all children receive special rights and protections during and after wartime, including those accused of having unlawfully engaged in wartime activities. International law severely restricts the recruitment and use of child soldiers, and in fact, may be moving towards abolishing their recruitment and use altogether.<sup>70</sup> The recruitment and use of all children under 15 years old to actively participate in hostilities is prohibited, as well as the forced or compulsory recruitment of children between 15-18 years old. Even if the latter join State armed forces voluntarily, they may not participate directly in hostilities; and, furthermore, international law imposes strict criteria to ensure that children give informed consent. Any enlistment in non-State armed groups is prohibited *per se*. As discussed in Part III, international law generally precludes the prosecution of child soldiers unless it serves a rehabilitative function. This is particularly true for child soldiers who have been unlawfully recruited and who should be viewed as victims of the conflict. Accordingly, their rehabilitation and reintegration into society should be any court’s primary concern.

---

<sup>67</sup> Laurence Steinberg & Robert Schwartz, *Developmental Psychology Goes to Court*, in *YOUTH ON TRIAL: A DEVELOPMENTAL PROSPECTIVE ON JUVENILE JUSTICE* 23 (Thomas Grisso & Robert Schwartz, eds., 2003); see also JOHN LAUB & ROBERT SAMPSON, *SHARED BEGINNINGS, DIVERGENT LIVES: DELINQUENT BOYS TO AGE 70* (2003).

<sup>68</sup> *Simmons*, *supra* note 59, at 570.

<sup>69</sup> *Id.*

<sup>70</sup> See, e.g., African Charter on the Rights and Welfare of the Child art. 22(2), O.A.U. Doc. CAB/LEG/24.9/49 (1990) (requiring that States Parties “ensure that no child shall take a direct part in hostilities and refrain in particular from recruiting any child”).

i. Presumption of Victimization

The prohibition of the recruitment and use of children under 15 to participate actively in hostilities is enshrined in treaty law as a rule of customary international law, and thus binding on the U.S.<sup>71</sup> In fact, the Geneva Protocols influenced the drafting of the CRC because most State participants viewed their provisions as reflecting customary international law.<sup>72</sup> Article 77 of Protocol I prohibits the recruitment of children under 15 years old into armed forces and their direct participation in hostilities in international armed conflicts.<sup>73</sup> Similarly, Article 4(3) of Protocol II prohibits the recruitment of children under 15 years old into armed forces and their direct participation in non-international armed conflicts.<sup>74</sup> Article 38(2) of the CRC, following suit, requires States Parties to ensure that persons who have not attained the age of fifteen years do not take a direct part in hostilities, and Article 38(3) likewise obliges States Parties to refrain from recruiting any person who has not attained the age of fifteen years into their armed forces.<sup>75</sup> Both Protocol I and the CRC require that in recruiting among children who have attained the age of 15, but who have not yet attained the age of 18, States Parties shall give priority to those who are oldest.<sup>76</sup>

For children between 15-18 years old, the Optional Protocol to the CRC on the Involvement of Children in Armed Conflict (“OPCRC”) requires States Parties to maintain minimum safeguards that ensure such recruitment is genuinely voluntary and is carried out with the informed consent of the child’s parents or guardians.<sup>77</sup> It also requires that such persons be informed of the duties involved and that they provide reliable proof of age prior to

---

<sup>71</sup> The Paquete Habana, 175 U.S. 677, 700 (1900) (holding that “[i]nternational law is part of our law, and must be ascertained and administered by the courts of justice of appropriate jurisdiction, as often as questions of right depending upon it are duly presented for their determination”).

<sup>72</sup> See, e.g., Michael Matheson, *The Sixth Annual American Red Cross-Washington College of Law Conference on International Humanitarian Law: A Workshop on Customary International Law and the 1977 Protocols Additional to the 1949 Geneva Conventions*, 2 AM. U. J. INT’L L. & POL’Y 415, 428 (1987) (explaining that while the U.S. was unwilling to ratify Protocol I, it viewed many provisions as reflecting customary international law, including the principle that children under fifteen should not take a direct part in hostilities).

<sup>73</sup> Protocol I, *supra* note 38, at art. 77.

<sup>74</sup> Protocol II, *supra* note 39, at art. 4(3).

<sup>75</sup> CRC, *supra* note 29, at art. 38.

<sup>76</sup> Protocol I, *supra* note 38, at art. 77(2); CRC, *supra* note 29, at art. 38(3).

<sup>77</sup> Optional Protocol to the Convention on the Rights of the Child on the Involvement of Children in Armed Conflict Annex I, art. 3, G.A. Res. 54/263, U.N. Doc. A/RES/54/49 (May 25, 2000) [hereinafter OPCRC].

enlistment.<sup>78</sup> All recruitment of child soldiers by non-State armed groups is presumed to be involuntary, and thus illegal. Non-State groups are prohibited from recruiting or using children under 18 years old "under any circumstances."<sup>79</sup> Of course, non-State groups cannot be parties to the OPCRC, so only States can monitor their activities. For that reason, Article 4(2) requires that States Parties take "all feasible measures to prevent such recruitment and use, including the adoption of legal measures necessary to prohibit and criminalize such practices."<sup>80</sup> The U.S. is one of many countries bound by this treaty.<sup>81</sup>

Unlawfully recruited children should be presumed victims of human rights violations, and possibly even as victims of war crimes. Many children are drugged, coerced, sexually exploited, and/or forced to commit atrocities during and after their recruitment.<sup>82</sup> The International Labor Organization considers the forced or compulsory recruitment of children for armed conflict to be a form of modern slavery.<sup>83</sup> Article 8(2) of the Rome Statute lists conscripting or enlisting children under 15 years old into armed forces or using them to participate actively in conflicts as war crimes within the ICC's jurisdiction.<sup>84</sup> Moreover, the Rome Statute was selectively incorporated into the SCSL Statute,<sup>85</sup> under which several persons were prosecuted for unlawfully recruiting child soldiers.<sup>86</sup> In the *Lubanga* case, the SCSL noted that unlawful conscription and enlistment are continuous in nature and only end when children reach the age of fifteen or leave the armed group.<sup>87</sup>

---

<sup>78</sup> *Id.*

<sup>79</sup> *Id.* at art. 4.

<sup>80</sup> *Id.*

<sup>81</sup> OPCRC Treaty Status available at <http://treaties.un.org/Pages/ViewDetails.aspx>.

<sup>82</sup> Graca Machel, *Promotion and Protection of the Rights of Children: Impact of Armed Conflict on Children*, U.N. Doc. A/51/306 (Aug. 26, 1996), available at [http://www.unicef.org/graca/a51-306\\_en.pdf](http://www.unicef.org/graca/a51-306_en.pdf).

<sup>83</sup> Convention Concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labor art 3., I.L.O. 182 (1999), available at <http://www.ilo.org/public/english/standards/relm/ilc/ilc87/com-chic.htm>.

<sup>84</sup> Rome Statute, *supra* note 45.

<sup>85</sup> See SCSL Statute, *supra* note 49, at art. 4(c).

<sup>86</sup> See, e.g., Prosecutor v. Hinga Norman, Decision on Preliminary Motion Based on Lack of Jurisdiction, ¶¶ 17-23, SCSL-04-14-AR72(E) (May 31, 2004) (finding that enlisting child soldiers had been prohibited in customary international law and subjected individuals to criminal responsibility before the Rome Statute's adoption), available at <http://www.scsl.org/LinkClick.aspx?fileticket=XSDlFGVsutI=&tabid=193>; Prosecutor v. Brima, Judgment, SCSL-04-16-T (June 20, 2007) (finding all defendants guilty of child recruitment), available at <http://www.refworld.org/docid/467fba742.html>; Prosecutor v. Fofana and Kondewa, Judgment, SCSL-04-14-T (Aug. 2, 2007) (finding the defendant Kondewa guilty of child recruitment), available at <http://www.scsl.org/LinkClick.aspx>.

<sup>87</sup> *Lubanga*, *supra* note 47, at ¶ 618 (citing Prosecutor v. Nahimana, Appeals Judgment, ¶ 721,

## ii. Rehabilitation and Reintegration

If a criminal tribunal seeks to exercise jurisdiction over a minor, it should view the child as a victim and do so with the goal of rehabilitating and reintegrating the child. The Principles and Guidelines on Children Associated with Armed Forces or Armed Groups (the Paris Principles) state that “at all stages,” the objective of programming should be to enable children “to play an active role as a civilian member of society, integrated into the community and, where possible, reconciled with her/his family.”<sup>88</sup> The CRC obliges States Parties to “take all appropriate measures to promote physical and psychological recovery and social reintegration” of neglected, exploited, tortured, or abused children.<sup>89</sup> Such recovery and reintegration should take place in an environment which fosters their health, self-respect, and human dignity.<sup>90</sup> The OPCRC further obliges States Parties to “take all feasible measures to ensure that such persons...are demobilized or otherwise released from service...[and] when necessary, [provide] all appropriate assistance” for their recovery and reintegration.<sup>91</sup>

The US ratified the OPCRC in December 2002<sup>92</sup> and has continuously recognized the importance of rehabilitative programs. An OPCRC report noted that the US contributed “substantial resources” to international programs aimed at preventing the recruitment of children and reintegrating child soldiers into society and “is committed to continue to develop rehabilitation approaches that are effective in addressing this serious and difficult problem.”<sup>93</sup> Specifically, the US noted that it contributed over \$10 million towards the demobilization of child soldiers and their reintegration in several countries, including Afghanistan.<sup>94</sup> These facts make Khadr’s seemingly retributive proceedings all the more surprising.

## iii. Immunity from Continuing Prosecution

As discussed in Part III, *infra*, children are less culpable for their actions

---

ICTR-99-52-A (Nov. 28, 2007), available at <http://www.refworld.org/docid/48b5271d2.html>).

<sup>88</sup> Principles and Guidelines on Children Associated with Armed Forces or Armed Groups § 7.0 (2007) [hereinafter Paris Principles], available at <http://www.unicef.org/emerg/files/ParisPrinciples310107English.pdf>.

<sup>89</sup> CRC, *supra* note 29, at art. 39.

<sup>90</sup> *Id.*

<sup>91</sup> OPCRC, *supra* note 78, at art. 6.

<sup>92</sup> See note 82.

<sup>93</sup> United States of America, *Initial Report to the U.N. Committee on the Rights of the Child on the Involvement of Children in Armed Conflict*, ¶ 34, U.N. Doc. CRC/C/OPAC/USA/1 (June 22, 2007), available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G07/426/17/PDF/G0742617.pdf>.

<sup>94</sup> *Id.* at ¶ 35.

due to their immaturity and decision-making. A person cannot, and should not, be held responsible for a crime if he or she was not fully responsible at the time he or she committed it. This notion was deliberately reflected in the drafting of the SCSL's statute, which protects all persons who committed crimes when they were children, regardless of their age when they appeared before the court.<sup>95</sup> Consequently, a defendant who is now an adult but was a child soldier at the time he or she allegedly committed war crimes should receive the same international protections as accused child soldiers.

### *B. Denial of Substantive Rights and Procedural Safeguards*

Prosecutions of minors should be viewed as a last resort,<sup>96</sup> and any prosecutions should comply with international juvenile standards.<sup>97</sup> (Of course, any minimum child-specific standards are in addition to safeguards guaranteed to all similarly situated defendants under international law.) Yet, in Khadr's case the U.S. government continued to try restricting his substantive rights and procedural safeguards. It is disturbing to consider the prospect that for many years Khadr was unable to exercise his fundamental rights and was arguably subjected to a "kangaroo court."

#### *i. Habeas Petitions*

Initially, President Bush's military order specified that detainees subject to it would have no access to the U.S. federal court system to appeal a verdict or obtain any other relief.<sup>98</sup> The U.S. Supreme Court later invalidated this order.<sup>99</sup> In response, Congress enacted the Detainee Treatment Act of 2005 ("DTA"). The DTA revoked all federal jurisdiction over habeas claims by persons detained as "enemy combatants," creating jurisdiction in the Court of Appeals for the DC Circuit to hear appeals of final decisions of military commissions.<sup>100</sup> The US Supreme Court again invalidated the military commissions system in the *Hamdan* case, holding that the commissions were required to follow procedural rules under the Uniform Code of Military Justice.<sup>101</sup>

Congress then passed the 2006 MCA, which attempted to strip the

<sup>95</sup> U.N. Security Council President, Letter dated Dec. 20, 2000 from the President of the Security Council addressed to the Secretary-General, *supra* note 51, Annex at art. 7.

<sup>96</sup> See, e.g., CRC, *supra* note 29, at art. 37(b); U.N. Rules for the Protection of Juveniles Deprived of Their Liberty art. 2, G.A. Res. 45/113 (Dec. 14, 1990) [hereinafter UN Rules].

<sup>97</sup> See, e.g., Paris Principles, *supra* note 89, at §§ 8.8, 8.9.0.

<sup>98</sup> Military Order of Nov. 13, 2001, 66 Fed. Reg. 57831, § 7(b), *available at* <http://www.fas.org/irp/offdocs/eo/mo-111301.htm>.

<sup>99</sup> *Rasul v. Bush*, 542 U.S. 466, 485 (2004).

<sup>100</sup> See 42 USC § 2000dd., Detainee Treatment Act of 2005, *available at* <http://uscode.house.gov/download/pls/42C21D.txt>.

<sup>101</sup> *Hamdan*, *supra* note 25.



judiciary of habeas jurisdiction in all cases brought by detainees, including pending cases.<sup>102</sup> The 2006 MCA also provided that, “[n]o alien unlawful enemy combatant subject to trial by military commission . . . may invoke the Geneva Conventions as a source of rights.”<sup>103</sup> Moreover, the 2006 MCA explicitly authorized the President to determine the meaning and application of the Geneva Conventions.<sup>104</sup> The U.S. Supreme Court again held that Congress’s actions were unconstitutional.<sup>105</sup> As Justice Kennedy explained, the Act undermined the rule of law and effectively prevented the judiciary from interpreting and applying the law: “Trial by military commission raises separation-of-powers concerns of the highest order. Located within a single branch, these courts carry the risk that offenses will be defined, prosecuted, and adjudicated by executive officials without independent review.”<sup>106</sup> The denial of any possibility of habeas relief contravened Khadr’s rights to challenge his detention before a court or other competent and independent authority, and to a prompt decision on any such action.<sup>107</sup>

## ii. Assistance of Counsel

Under the CRC, every child deprived of his or her liberty is entitled to prompt access to legal and other appropriate assistance.<sup>108</sup> Khadr did not receive access to legal counsel until more than two years after he was transferred to Guantánamo.<sup>109</sup> The 2006 MCA also restricted a defendant’s right to choose his own attorney. Detainees could only be represented by U.S. civilian attorneys and their assigned military defense attorney.<sup>110</sup> Many detainees such as Khadr are likely suspicious of U.S. attorneys and would rather be represented by counsel from their home country. Also, the 2006 MCA only provided a right to counsel after the swearing of charges,<sup>111</sup> which meant that the U.S. government could delay charging a detainee to conduct interrogations in the absence of counsel. Finally, defense counsel was restricted in its ability to see and discuss certain information with its clients.<sup>112</sup>

<sup>102</sup> See 2006 MCA, *supra* note 26, at § 7.

<sup>103</sup> *Id.* at § 948b(g).

<sup>104</sup> *Id.* at § 950w.

<sup>105</sup> *Boumediene v. Bush*, 553 U.S. 723, 798 (2008).

<sup>106</sup> *Hamdan*, *supra* note 25, at 638.

<sup>107</sup> See CRC, *supra* note 29, at art. 37(d); ICCPR, *supra* note 56, at art. 9(4).

<sup>108</sup> CRC, *supra* note 29, at art. 37(d), 40(2).

<sup>109</sup> Human Rights First, *Omar Ahmed Khadr*, available at <http://www.humanrightsfirst.org/our-work/law-and-security/military-commissions/cases/omar-ahmed-khadr/>.

<sup>110</sup> 2006 MCA, *supra* note 26, at § 949c(b)(3-5).

<sup>111</sup> *Id.* at § 948k.

<sup>112</sup> *Id.* at § 949p-4(a-b).

### iii. Evidentiary Issues

#### *a. Reliability*

Under the 2006 MCA, confessions or other statements of the accused elicited through coercion, compulsory self-incrimination, or any cruel, inhuman, or degrading treatment could be admissible at trial,<sup>113</sup> without *Miranda* warnings being provided first.<sup>114</sup> The statements' admissibility depended on when they were made. Prior to the DTA's enactment, coercion that did not amount to torture was admissible if (1) under the "totality of circumstances" under which any statements were made, they were reliable and had sufficient probative value; and (2) "the interests of justice" would be served by their admission.<sup>115</sup> After the DTA's enactment, such statements were admissible if the interrogation methods used to obtain them did not violate the cruel or unusual punishment amendments to the U.S. Constitution.<sup>116</sup> Enhanced interrogation techniques such as waterboarding were not expressly barred, which plainly ignored the international prohibition on such techniques.

The MCA's allowances are especially significant in light of juvenile propensity to give false confessions. Various studies have shown that juveniles do not understand or appreciate *Miranda* warnings as well as adults.<sup>117</sup> Children may also comply with interrogators' demands due to their vulnerability and societal expectations that they respect authority.<sup>118</sup> Khadr claimed that he was subjected to many enhanced interrogations without forewarning, and that he would often give false responses if he believed the interrogations might end.<sup>119</sup>

#### *b. Accessibility*

Under the MCA, classified information is protected during all stages of proceedings and privileged from disclosure for purported national security

---

<sup>113</sup> *Id.* at § 949a(b)(2)(C).

<sup>114</sup> *Id.* at § 948b(d).

<sup>115</sup> *Id.* at § 948r.

<sup>116</sup> *Id.*

<sup>117</sup> See, e.g., Thomas Grisso, *Juveniles' Capacities to Waive Miranda Warnings: An Empirical Analysis*, 68 CALIF. L. REV. 1134, 1166 (1980).

<sup>118</sup> See Barry Feld, *Competence, Culpability, and Punishment: Implications of Atkins for Executing and Sentencing Adolescents*, 32 HOFSTRA L. REV. 463, 532 (2003); see also Gerald Robin, *Juvenile Interrogation and Confessions*, 10 J. POL. SCI. & ADMIN. 224, 225 (1982).

<sup>119</sup> Omar Khadr, Affidavit of Omar Ahmed Khadr (Feb. 22, 2008) [hereinafter Affidavit], available at [http://humanrights.ucdavis.edu/projects/the-guantanamo-testimonials-project/testimonies/prisoner-testimonies/omar\\_khadr\\_affidavit\\_22\\_feb\\_08.pdf](http://humanrights.ucdavis.edu/projects/the-guantanamo-testimonials-project/testimonies/prisoner-testimonies/omar_khadr_affidavit_22_feb_08.pdf).

concerns.<sup>120</sup> It is thus difficult for defendants to challenge certain evidence, because they may be denied access to information necessary to make the challenge. For example, though hearsay could be excluded under the 2006 MCA, the burden was on the defendant to clearly demonstrate that the evidence was unreliable or lacking in probative value.<sup>121</sup> But to test its reliability, defendants would have needed access to the sources, methods, or activities by which the information was obtained. Due to the nature of defendants' confinement and limited access to attorneys, conducting proper investigations has been rather difficult.

If certain information is deemed classified, then documents given to the accused are redacted or substituted. Some documents are not provided to the accused at all. The military judge must consider any claim of privilege and review supporting materials in camera, and is forbidden from disclosing the privileged information.<sup>122</sup> The MCA does not explicitly provide an opportunity for the accused to contest the admissibility of substitute evidence, nor does it seem to allow the accused or defense counsel to examine the proffered evidence prior to its presentation to the commission.

### C. *Unlawful Detention*

International law requires that any juvenile detention be an exceptional measure that takes into account the needs of persons his or her age.<sup>123</sup> Specifically, the International Committee for the Red Cross ("ICRC") urges authorities to take the following measures regarding detained children: administer questioning without delay; detain the children in quarters separate from adults; for extended detention, transfer child detainees to institutions that specialize in care for minors; provide food, hygiene, and medical care that is suitable to the age and condition of each child; allow them to spend most of their time outdoors; allow them to continue their education; and ensure regular contact with their families.<sup>124</sup> The facts of Khadr's case clearly indicate that he was subjected to unlawful detention, in terms of both its duration and conditions.

---

<sup>120</sup> See MCA, *supra* note 29, at § 948a(4) (defining "classified information" as "[a]ny information or material that has been determined by the United States Government pursuant to statute, Executive order, or regulation to require protection against unauthorized disclosure for reasons of national security" and "restricted data, as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y))").

<sup>121</sup> 2006 MCA, *supra* note 26, at § 949a(b)(2)(E).

<sup>122</sup> *Id.* at § 949d(f)(3).

<sup>123</sup> CRC, *supra* note 29, at art. 37.

<sup>124</sup> International Committee of the Red Cross ("ICRC"), *Children in War* 14 (Nov. 2009), available at [http://www.icrc.org/eng/assets/files/other/icrc\\_002\\_4015.pdf](http://www.icrc.org/eng/assets/files/other/icrc_002_4015.pdf).

### i. Duration

Under the MCA, detainees do not have the right to a speedy trial;<sup>125</sup> however, several international instruments contradict that position. The CRC provides that juvenile detention shall be “for the shortest appropriate period of time,”<sup>126</sup> and that juvenile cases shall be heard “without delay.”<sup>127</sup> Similarly, the ICCPR states that juveniles shall be brought “as speedily as possible” for adjudication.<sup>128</sup> Khadr was detained for over two years before he was formally charged.<sup>129</sup> By the time of his plea agreement, he had been detained for over eight years (see Part V, *infra*).

### ii. Conditions

#### a. *Minimum Standards*

The ICCPR, which the U.S. has ratified,<sup>130</sup> prohibits any cruel, inhuman, or degrading treatment,<sup>131</sup> and requires that detainees be treated “with humanity and respect for [their] inherent dignity.”<sup>132</sup> Common Article III of the Geneva Conventions, which is recognized as customary international law, similarly provides safeguards against cruel treatment, torture, and “outrages upon personal dignity, in particular, humiliating and degrading treatment.”<sup>133</sup> It also states that the “wounded and sick shall be collected and cared for.”<sup>134</sup> Khadr stated that he was badly wounded in the firefight with U.S. soldiers and did not receive proper medical treatment.<sup>135</sup> He also claimed that on numerous occasions, U.S. and Canadian authorities improperly interrogated him, aggravated his injuries, or mistreated him in other ways.<sup>136</sup> Such actions, if true, would have unquestionably breached minimum international safeguards.

<sup>125</sup> MCA, *supra* note 28, at § 948b(d).

<sup>126</sup> CRC, *supra* note 29, at art. 37(b); UN Rules, *supra* note 97, at art. 2.

<sup>127</sup> CRC, *supra* note 29, at art. 40(2).

<sup>128</sup> ICCPR, *supra* note 56, at art. 10(2).

<sup>129</sup> Human Rights Watch, *Omar Ahmed Khadr* (Oct. 25, 2012) [hereinafter HRW], *available at* <http://www.hrw.org/news/2012/10/25/omar-ahmed-khadr>.

<sup>130</sup> ICCPR Treaty Status *available at* [http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg\\_no=IV-4&chapter=4&lang=en](http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en).

<sup>131</sup> ICCPR, *supra* note 56, at art. 7.

<sup>132</sup> *Id.* at art. 10(1).

<sup>133</sup> Common Article III of the Four Geneva Conventions (1949).

<sup>134</sup> *Id.*

<sup>135</sup> Affidavit, *supra* note 120.

<sup>136</sup> *Id.*

### *b. Child-Specific Standards*

International law provides that every child in detention shall be separated from adults,<sup>137</sup> except in the unusual event that it is not in the child's best interest to do so.<sup>138</sup> Khadr, however, was detained with the adult population at Guantánamo starting when he was 16 years old and remained there until his release.<sup>139</sup> According to the CRC, detained children also have the right to maintain regular contact with their family through correspondence and visits.<sup>140</sup> Khadr was allowed to speak to his family on the phone only once after five years of detention,<sup>141</sup> and it is likely that he was forbidden from seeing his family in person. Detained children also have rights to education and recreation,<sup>142</sup> and should have access to specialized juvenile justice systems, with specially trained judges, prosecutors and attorneys.<sup>143</sup> U.S. authorities never made any of these things available to Khadr, nor did he ever have an opportunity to request that his case be transferred to a different forum.

## V. PLEA AGREEMENT & SENTENCE

### *A. Overview*

Khadr entered into a plea agreement with the U.S. government in 2010.<sup>144</sup> In exchange for a sentence of eight years or fewer on all charges,<sup>145</sup> Khadr would not receive any credit for time already served in U.S. custody.<sup>146</sup> Furthermore, he would have to serve at least one more year at Guantánamo.<sup>147</sup> The U.S. government also failed to give assurances regarding his repatriation to Canada thereafter,<sup>148</sup> which was somewhat troubling because the U.S. government would not allow him into its territory.<sup>149</sup> Many

<sup>137</sup> ICCPR, *supra* note 56, at art. 10(2); CRC, *supra* note 29, at art. 37(c).

<sup>138</sup> CRC, *supra* note 29, at art. 37(c).

<sup>139</sup> HRW, *supra* note 130.

<sup>140</sup> CRC, *supra* note 29, at art. 37(c).

<sup>141</sup> *Canadian Guantanamo Detainee Calls Home*, CBC NEWS CANADA (updated Mar. 8, 2007), <http://www.cbc.ca/news/canada/story/2007/03/08/khadrspeaks.html>.

<sup>142</sup> See U.N. Standard Minimum Rules for the Administration of Juvenile Justice art. 13.5, G.A. Res. 40/33 (Nov. 29, 1985) [hereinafter "Beijing Rules"]; U.N. Rules, *supra* note 97, at art. 18(b)(c), 38, 47.

<sup>143</sup> Beijing Rules, *supra* note 143, at art. 6.3, 22.1.

<sup>144</sup> *United States v. Khadr*, Offer for Pre-trial Agreement (Oct. 13, 2010), ¶ 4 [hereinafter *Plea Agreement*], available at <http://www.mc.mil/CASES/MilitaryCommissions.aspx>.

<sup>145</sup> *Id.* at ¶ 6(a).

<sup>146</sup> *Id.* at ¶ 2(e).

<sup>147</sup> *Id.* at ¶ 5(h).

<sup>148</sup> *Id.*

<sup>149</sup> *Id.* at ¶ 2(k).

denounced the plea agreement, including Khadr's Canadian attorney, who called it a "piece of paper" and also stated that Khadr "would have confessed to anything . . . just to get out of [that] hellhole."<sup>150</sup> Khadr was 24 years old when he was sentenced to eight more years in prison.<sup>151</sup> Various organizations petitioned for Khadr's repatriation to Canada.<sup>152</sup> He was later repatriated, where he is currently serving the remainder of that sentence.<sup>153</sup>

## B. Assessment

### i. The Plea Agreement

The circumstances surrounding Khadr's plea agreement are highly questionable. Even though Khadr stipulated to the U.S. government's facts and relinquished certain critical rights "voluntarily,"<sup>154</sup> one should not presume that he genuinely agreed on that basis. The U.S. government had a substantial amount of leverage in the plea negotiations with Khadr, and as his Canadian attorney noted, he would have confessed to virtually anything.<sup>155</sup> Even though Khadr was 24 years old when he entered into the agreement, he had been in custody for about eight years in substandard conditions, and charges against him had already been dropped.<sup>156</sup> There was no clear end in sight. By rejecting the plea agreement, Khadr would have borne the risk of reinstated charges, an unfair trial, or perhaps worst of all, indefinite detention.

### ii. The Sentence

Notwithstanding Khadr's objectionable status review, detention, and plea agreement, his final sentence was comparable to—and in some instances, better than—other similarly situated juvenile defendants in the U.S. and abroad.<sup>157</sup>

<sup>150</sup> *Khadr to Return to Canada: Lawyer*, CBC NEWS CANADA (updated Oct. 25, 2010), <http://www.cbc.ca/news/world/story/2010/10/25/omar-khadr-trial-resumes.html>.

<sup>151</sup> *Omar Khadr Sentenced to Symbolic 40 years*, CBC NEWS CANADA (updated Oct. 31, 2010), <http://www.cbc.ca/news/world/story/2010/10/31/guantanamo-khadr-sentencing.html>.

<sup>152</sup> See, e.g., Amnesty International Canada, *Omar Khadr: Repatriation to Canada is the Only Option!*, Action Alert, available at <http://www.globalresearch.ca/omar-khadr-repatriation-to-canada-is-the-only-option/17399>.

<sup>153</sup> CBC report, *supra* note 2.

<sup>154</sup> Plea Agreement, *supra* note 145, at ¶ 2(c).

<sup>155</sup> See also Part IV (B)(3)(a), *infra*, discussing the propensity of juveniles to falsely confess to crimes.

<sup>156</sup> *Guantanamo Judge Drops Charges Against Khadr*, CBC NEWS CANADA (updated June 4, 2007), available at <http://www.cbc.ca/news/world/story/2007/06/04/khadr-charges.html>.

<sup>157</sup> The following Section does not seek to address the legality of the death penalty under international law, nor to critique States that have chosen to retain or abolish it from their domestic legislation.

*a. American Perspective*

In the U.S., the Federal Juvenile Delinquency Act (“FJDA”) would have applied to Khadr’s case.<sup>158</sup> Under the FJDA, a juvenile offender must be sentenced according to his or her age at the time of sentencing.<sup>159</sup> Because Khadr was 24 years old at the time of sentencing, he would have been properly sentenced as an adult.<sup>160</sup> Under federal law, adults are subject to the death penalty for war crimes that result in the death of a victim;<sup>161</sup> however, the U.S. Supreme Court has held that juvenile defendants under 16 years old at the time of the alleged offense are exempt from the death penalty.<sup>162</sup> Khadr’s maximum prison sentence also could not have exceeded that of a similarly situated adult.<sup>163</sup> While the Federal Sentencing Guidelines are not mandatory,<sup>164</sup> courts may still need to apply them in determining a maximum possible term of imprisonment. Using the Guidelines worksheets,<sup>165</sup> one finds that Khadr’s sentence by the military commission was comparable to any sentence he might have received in a US district court.

*b. Comparative Perspective*

According to the ICRC, sentencing systems for war crimes vary widely among States.<sup>166</sup> Some countries impose the most severe sentence regardless of the war crime; sentences range from the death penalty,<sup>167</sup> to life imprisonment,<sup>168</sup> to lifelong penal servitude.<sup>169</sup> Other countries distinguish

---

<sup>158</sup> See 18 USC § 5031, Federal Juvenile Delinquency Act (defining “juvenile delinquency” as a violation of U.S. law committed by a person prior to his eighteenth birthday, which would have been a crime if committed by an adult) [hereinafter FJDA], *available at* <http://uscode.house.gov/download/pls/18C403.txt>.

<sup>159</sup> See, e.g., *United States v. Leon H.*, 365 F.3d 750, 753 (9th Cir. 2004); *United States v. K.R.A.*, 337 F.3d 970, 977 (8th Cir. 2003).

<sup>160</sup> See FJDA, *supra* note 158, at § 5037(c).

<sup>161</sup> 18 USC § 2441(a), War Crimes Act, *available at* <http://uscode.house.gov/download/pls/18C118.txt>.

<sup>162</sup> *Thompson v. Oklahoma*, 487 U.S. 815, 838 (1988).

<sup>163</sup> See, e.g., *United States v. A.J.*, 190 F.3d 873, 875 (8th Cir. 1999) (interpreting the FJDA).

<sup>164</sup> *United States v. Booker*, 543 U.S. 220, 264 (2005).

<sup>165</sup> Sentencing Guidelines Worksheets *available at* [http://www.uscc.gov/Education\\_and\\_Training/Guidelines\\_Worksheets/Worksheets\\_for\\_Individuals.pdf](http://www.uscc.gov/Education_and_Training/Guidelines_Worksheets/Worksheets_for_Individuals.pdf).

<sup>166</sup> ICRC, *Analysis of the Punishments Applicable to International Crimes (War Crimes, Crimes Against Humanity and Genocide) in Domestic Law and Practice*, 90 ICRC REV. 461, 464 (2008) [hereinafter ICRC Article], *available at* [http://www.icrc.org/eng/assets/files/other/irrc-870\\_reports-and-documents.pdf](http://www.icrc.org/eng/assets/files/other/irrc-870_reports-and-documents.pdf).

<sup>167</sup> *Id.* (citing Burundi, Congo, Côte d’Ivoire and Mali as examples).

<sup>168</sup> *Id.* (citing Congo as an alternative to capital punishment).

<sup>169</sup> *Id.* (citing Democratic Republic of the Congo as an example).

between fatal and non-fatal war crimes. The U.S., Nigeria, and India impose the death penalty for fatal crimes, though the death penalty for juveniles is almost universally condemned in law,<sup>170</sup> and State practice.<sup>171</sup> Uganda, Canada, and the UK, only impose life imprisonment.<sup>172</sup> Some modern post-conflict States, such as Rwanda, have more detailed sentencing scales for war crimes.<sup>173</sup> Rwanda was also the first country to hold individuals accountable for war crimes committed when they were minors,<sup>174</sup> though the Rwandan government has also allowed for mitigating circumstances.<sup>175</sup>

## VI. CONCLUSIONS & RECOMMENDATIONS

Despite Khadr's objectionable status review, detention, and plea agreement under the military commissions system, his final sentence was at least proportionate to the war crimes he allegedly committed. More importantly though, Khadr's case reminds the international community that children need to be held accountable for their actions. Specifically, child soldiers should be held as accountable for their actions on the battlefield as their adult commanders. But what exactly does "accountable" mean in this sensitive context?

<sup>170</sup> CRC, *supra* note 29, at art. 37(a); ICCPR, *supra* note 56, at art. 6(5); Beijing Rules, *supra* note 143, at art. 17.2.

<sup>171</sup> See, e.g., Amnesty International, *The World Moves Towards Abolition* (2013), available at <http://www.amnestyusa.org/our-work/issues/death-penalty/international-death-penalty>. Yet, child soldiers are still executed around the world; See, e.g., Child Soldiers International, *Child Soldiers Global Report – Congo, Democratic Republic of the* (2004) (where several child soldiers were tried and summarily executed for alleged murder by military courts), available at <http://www.refworld.org/docid/49880668c.html>; *Two child soldiers facing execution*, DEMOCRATIC VOICE OF BURMA (Oct. 16, 2009) (where two child soldiers faced execution for alleged murder), available at <http://www.dvb.no/news/two-child-soldiers-facing-execution/2978>.

<sup>172</sup> ICRC Article, *supra* note 166, at 464.

<sup>173</sup> See *Repressing the Crime of Genocide, Crimes against Humanity and War Crimes*, Law No. 33 bis/2003 (Sept. 6, 2003) available at [http://www.geneva-academy.ch/RULAC/pdf\\_state/Law-33bis-2003-Crimes-Genocide-cah-war.pdf](http://www.geneva-academy.ch/RULAC/pdf_state/Law-33bis-2003-Crimes-Genocide-cah-war.pdf).

<sup>174</sup> See *Setting Up "Gacaca Jurisdictions" and Organizing Prosecutions for Offences Constituting the Crime of Genocide or Crimes Against Humanity Committed Between Oct. 1, 1990 and Dec. 31, 1994* art. 74, Organic Law No. 40/2000 (Jan. 26, 2001) (mandating prison sentences for individuals between 14-18 years old at the time of commission, and placement in "rehabilitation centers" for persons under 14 years old), available at <http://www.unhcr.org/refworld/docid/452e37514.html>.

<sup>175</sup> See *Establishing the Organisation, Competence, and Functioning of Gacaca Courts Charged with Prosecuting and Trying the Perpetrators of the Crime of Genocide and Other Crimes against Humanity, Committed between Oct. 1, 1990 and Dec. 31, 1994* art. 16, Organic Law No. 10/2007 (Mar. 1, 2007), *modifying* Organic Law No. 16/2004 (June 19, 2004), available at [http://www.geneva-academy.ch/RULAC/pdf\\_state/2007-Gacaca-Crts-Organic-Law-10-2007-3-languages-.pdf](http://www.geneva-academy.ch/RULAC/pdf_state/2007-Gacaca-Crts-Organic-Law-10-2007-3-languages-.pdf).



As discussed in Part III, *infra*, international law views children—owing to their immaturity and lack of experience—as particularly vulnerable, and that child soldiers are often victims of a larger scheme arising from their political, social, or economic circumstances. Accordingly, children are entitled to greater protections under the law and should receive treatment in accordance with those standards. This recognition does not imply, however, that children should not be held accountable at all. Failure to hold children accountable could have devastating consequences, such as commanders delegating their most atrocious tasks to children. This lack of accountability may allow commanders to escape superior liability, thereby indirectly continuing to expose children to the same risks from which the international community is trying to protect them. For this reason, governments *should* hold them accountable, but as a general rule, in a different way than adults.

Of course, the appropriate form of accountability will have to be determined on a case-by-case basis and should not depend on age alone. Some children join armed groups voluntarily and are clearly in control of their actions, not having been coerced, drugged, or forced to commit atrocities. For those children that commit the most heinous crimes and thus require the greatest attention, I propose the creation of a specialized international juvenile chamber within the ICC. The chamber would consist of highly trained judges, attorneys, and investigators in the field of international juvenile justice and would thus be better equipped to address children's needs than the current alternatives. The vast majority of child soldiers, however, do not fall into that category. As such, it is important to keep in mind that accountability does not necessarily require criminal proceedings, and other options, considered below, exist that may be in the best interests of a particular child.

In light of these considerations, Khadr's sentence was appropriate but does not justify the means used (see Part IV, *infra*). Military courts are generally inappropriate for trying civilian offenders, and the CRC Committee has urged that children be exempt from military tribunals.<sup>176</sup> Due to national security concerns, military hearings are often conducted "in camera" and may not be independent and impartial. Juvenile justice standards, due process safeguards, and adequate detention conditions are usually not guaranteed.<sup>177</sup> Finally, children frequently lack assistance of counsel or their parents or

---

<sup>176</sup> United States of America, *Concluding Observations: Rep. Submitted under OPCRC art. 8*, ¶¶ 29-30, U.N. Doc. CRC/C/OPAC/USA/CO1 (June 25, 2008), available at <http://www2.ohchr.org/english/bodies/crc/docs/co/CRC.C.OPAC.USA.CO.1.pdf>.

<sup>177</sup> Special Representative of the Secretary-General Ms. Radhika Coomaraswamy, *Statement on the Occasion of the Trial of Omar Khadr before the Guantánamo Military Commission* (Aug. 9, 2010), available at <http://childrenandarmedconflict.un.org/statements/9-august-2010-trial-of-omar-khadr/>.

guardians, and may not have access to the charges brought against them. Military courts are not required to treat children's best interests as their primary concern—contrary to the object and purpose of the CRC—and thus are inappropriate for trying children. Most of these shortcomings were apparent in Khadr's case and should be avoided at all costs in future cases.

Even if States insist upon using military proceedings, they can take certain measures to ensure that children's rights are protected. Governments should periodically review their domestic laws to ensure that detention occurs only where children pose a serious security risk, as a last resort, for the least amount of time possible, and in accordance with juvenile-appropriate standards under international law. States should also ensure that children have access to their parents or guardians and competent legal representation. Governments should seek to provide viable alternatives to detention, prosecution, or other punitive measures whenever possible, such as restorative justice mechanisms and community-based diversion programs aiming at the rehabilitation and reintegration of children into society.

The futures of delinquent children like Omar Khadr are defined by their brief but formative experiences with judicial systems. Whether those experiences positively change their lives depends on the actions of national governments, which have a legal and moral obligation to serve children's best interests. Regrettably, the U.S. has failed to ratify the CRC to date,<sup>178</sup> and should do so immediately for its own sake and the sake of children around the world. As a policy matter, the U.S.'s reputation and credibility in international discussions concerning children have suffered because of its failure. 193 countries have ratified or acceded to the CRC, and the U.S. joins Somalia as the only two countries in the world that have not.<sup>179</sup> As discussed in Part IV, *infra*, several CRC articles are especially important for safeguarding children's rights in criminal proceedings. Ratification would help ensure that all children, especially those like Omar Khadr, can exercise their basic rights.



---

<sup>178</sup> CRC Treaty Status *available at* <http://treaties.un.org/pages/viewdetails.aspx>.

<sup>179</sup> *Id.*

## STUDENT NOTE

### Cyber Utilities Infrastructure and Government Contracting

Corey P. Gray<sup>\*</sup>

#### Abstract

*The utilities critical infrastructure of the United States is under cyber attack and there is no plan in place to defend it. Hyper-technical phrases like “critical infrastructure” and “cyber security” often trigger muted responses, but the threat that America now faces is serious and deserves focused attention. This note takes a critical view of the deficiencies in the U.S.’s cyber security posture. It will specifically address the most pressing area, privately operated public utilities. The utilities sector provides essential services that impact the lives of every American. That sector increasingly relies on cyber systems to increase both their efficiency and profit margins. Most would agree that such reliance has improved the utilities sector. The problem, however, is that a lack of cyber security makes the sector vulnerable to potentially debilitating attacks. An attack that overrides a dam, electric grid, or nuclear facility would have a catastrophic impact on the country.*

*Congress has attempted to tackle the cyber security problem for over a decade. The obstacles posed by creating coherent cyber security are significant. At the center of the issue is a constitutional battle between civil liberties and public safety. While Congress struggles to reconcile those two competing interests, administrative agencies have the ability to implement stopgap defense measures. This note promotes using administrative agency contracting as an intermediate step towards shoring up the nation’s cyber defense. There exists a cogent framework for public safety regulation of utilities through contracting. All government utility contracts have physical security and safety requirements. Through contracting, administrative agencies can require utilities companies to adhere to cyber security standards in the same way they require physical security standards. This stopgap solution would provide much needed support to a vulnerable area of national defense. Failure to act spells disaster for the U.S. in this new cyber age.*

---

<sup>\*</sup> University of Miami School of Law, Class of 2014. Special thanks to Professor William Widen for supervising this writing project.

## Table of Contents

---

I. INTRODUCTION.....	153
II. UTILITIES CRITICAL INFRASTRUCTURE.....	156
A. <i>Increased Attacks</i> .....	156
B. <i>Market Insulation</i> .....	156
C. <i>Calls For Action</i> .....	158
III. THE ROLE OF CONGRESS IN FINDING A SOLUTION.....	159
A. <i>Cyber Security Legislation</i> .....	159
B. <i>Providing Security</i> .....	159
C. <i>2013 Cyber Security Legislation</i> .....	160
D. <i>The Fourth Amendment</i> .....	160
E. <i>Learning from Past Failures</i> .....	161
F. <i>The Public-Private Relationship is Essential</i> .....	162
G. <i>Avoiding Reactionary Measures</i> .....	162
IV. PATCHWORK SOLUTIONS.....	163
A. <i>Administrative Agency Solutions</i> .....	163
B. <i>The Department of Homeland Security</i> .....	163
i. <i>Recruiting Future Cyber Warriors</i> .....	163
ii. <i>Addressing Current Threats to Utilities</i> .....	164
iii. <i>Severity of the Threat</i> .....	165
V. CONTRACTING A STOPGAP FROM THE EXISTING UTILITIES FRAMEWORK.....	166
A. <i>How Contracting Can be Effective</i> .....	166
B. <i>Using Preexisting Contract Frameworks</i> .....	166
i. <i>Two Potential Approaches</i> .....	167
VI. CONSEQUENCES OF FAILING TO ACT.....	168
A. <i>Attacks in Perspective</i> .....	168
B. <i>Cyber Attack on Georgia</i> .....	169
C. <i>Cyber Attacks in the Future</i> .....	169
VII. CONCLUSION.....	170

## I. INTRODUCTION

“If the enemy opens the door, you must race in.”—Sun Tzu<sup>1</sup>

The cyber systems that control the U.S.’s critical infrastructure are under attack. To date, cyber systems have made U.S. critical infrastructure more efficient and effective. With the click of a mouse, an automated control system can regulate water flow to a dam, or electricity to a town. As a result, the U.S. has become reliant on cyber systems, particularly private-operated public utilities.<sup>2</sup> The increased reliance on these systems has made them vulnerable to cyber attacks.<sup>3</sup> Cyber aggressors target the U.S.’s utilities critical infrastructure (“utilities”) to steal, deny, and destroy its capabilities. Today, sophisticated cyber aggressors launch attacks while remaining largely unidentified and undetected. The concern is that a coordinated attack could expose whole sections of the population to the risk of war-like harm without firing a single bullet.<sup>4</sup> This concern grows daily as the U.S.’s reliance on cyber systems outpaces its cyber security posture. There is no national cyber defense in place to protect U.S. critical infrastructure cyber systems.<sup>5</sup> This unacceptable situation must be resolved.

Congress is the only governmental body that can establish a comprehensive cyber defense. Yet, it has failed to pass legislation to protect the cyber systems that control the nation’s critical infrastructure. The challenges that Congress faces in creating a cyber defense network are formidable. The core issue is establishing a balance between civil liberties and public safety. Although Congress has worked for over a decade to find a solution, no legislation has materialized. Congress must work to inform the public of the threat cyber attacks pose to private businesses, as well as to the government. The private companies that make up much of the nation’s critical infrastructure are a key component. These businesses have unique intergovernmental relationships. They are the U.S.’s front line of defense against cyber attacks. When they are attacked, the nation suffers. These businesses must be protected. They must also be informed of the threats cyber attacks pose to them and the nation.

Privately owned utilities are vulnerable to cyber attacks. Utility companies

---

<sup>1</sup> Sun Tzu, *THE ART OF WAR* 92 (Lionel Giles trans., Dover Publications Inc. 2002).

<sup>2</sup> Janet Napolitano, Sec’y, Dep’t of Homeland Security, Remarks at the San Jose State Univ. Interdisciplinary Cybersecurity Program (Apr. 16, 2012), <http://www.dhs.gov/news/2012/04/16/remarks-secretary-janet-napolitano-san-jose-state-university>.

<sup>3</sup> *Id.*

<sup>4</sup> Tzu, *supra* note 1, at 48.

<sup>5</sup> David A. Fulghum, *Russia Recruited Civilians For Cyber Attacks On Georgia*, AEROSPACE DAILY & DEF. REPORT, Aug. 26, 2009, at 4.

leverage cyber control systems for the benefits, but often fail to implement basic security measures for their own protection.<sup>6</sup> Where increased vulnerability would generally force businesses to secure themselves, utilities remain largely unchanged. This is in large part because public-private relationship between utilities and the government makes them resistant to traditional market pressures.<sup>7</sup> Utility companies have traditionally had government protections that insulate them from the market.<sup>8</sup> Additionally, liability claims against utilities are generally subject to choice of law rules that further insulate them from liability suits.<sup>9</sup> As a result, utilities have little incentive to enhance their cyber security posture. These factors create fertile conditions for cyber attacks.

Utilities infrastructure is a blind spot in the nation's cyber defense. In order to understand and prevent threats, the government must be able to analyze attacks before, during, and after they happen. Public-private cooperation is a critical component to developing a coherent cyber defense.<sup>10</sup> The U.S. government cannot force private companies to disclose information on attacks to cyber systems. Yet, in order to achieve the requisite level of responsiveness, the government must be informed about current and future threats. The government must be able to identify threats and trends with enough time to respond. Requiring companies to grant government access would infringe upon civil liberties. If it facilitates an environment of information sharing, private companies can simply decline to participate. Striking the balance between civil liberties and public safety has created gridlock in Congress over how to cover this blind spot in cyber defense.

Administrative agency officials have grown impatient with the lack of cyber defense legislation. As a result, they have begun engaging the public directly about the need for a national cyber security strategy.<sup>11</sup> Administrative agencies are also implementing their own patchwork solutions to curb the impact of

---

<sup>6</sup> David Goldman, *Hacker Hits on U.S. Power and Nuclear Targets Spiked in 2012*, CNN MONEY (January 9, 2013, 1:41 PM),

<http://money.cnn.com/2013/01/09/technology/security/infrastructure-cyberattacks>.

<sup>7</sup> *GMC v. Tracy*, 519 U.S. 278, 289-90 (1997) (stating that regulated monopolies are consistent with the commerce clause), *see also* *Panhandle Eastern Pipe Line Co. v. Michigan Pub. Serv. Comm'n*, 341 U.S. 329, 333 (stating that public utilities sold to local private and industrial customers is generally regulated by states).

<sup>8</sup> *GMC*, 519 U.S. at 289-90.

<sup>9</sup> 28 U.S.C. §1346(b)(1), *see also* *Richards v. United States*, 369 U.S. 1, 10, (1962) (stating that the choice of law rules in state where negligence occurred apply to claims for damages).

<sup>10</sup> Michael Bruno, *Pentagon Nears Completion Of New Cyber Rules Of Engagement*, AEROSPACE DAILY & DEF. REPORT, Jun. 28, 2013, at 6.

<sup>11</sup> Leon Panetta, Sec'y, Dep't of Def., Remarks at the Bus. Execs. for Nat'l Sec. (Oct. 11, 2012), <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136>.

cyber threats. The Department of Homeland Security (the “DHS”), in particular, has implemented several innovative programs.<sup>12</sup> To address future threats, DHS has initiated a cyber warrior recruiting campaign on college campuses.<sup>13</sup> To address current threats, it has initiated programs based on public-private information sharing.<sup>14</sup> Although these agency programs are addressing the cyber threat and reducing the impact of cyber attacks, more must be done.

Administrative agencies should require all utility companies with government contracts to maintain a minimum level of cyber security. Cyber security requirements could seamlessly be incorporated into this well-worn framework. A minimum cyber security requirement would allow the current utilities scheme to remain intact. Contracting could be used to leverage the unique public-private relationship to its advantage. The federal government currently requires utilities to adhere to security and safety standards.<sup>15</sup> Specific cyber security requirements can be monitored much like physical security requirements. This minimum requirement would also reduce the government’s need for information on attacks, allowing it to focus on significant threats and trends. A minimum level of cyber security in utilities would mitigate coordinated cyber attacks. The result would yield a minimum cyber defense for the most vulnerable critical infrastructure sector.

The consequences for failing to prepare for cyber warfare are a dire. The Russian invasion of Georgia is one example of how cyber attacks will likely be employed in the near future.<sup>16</sup> There, coordinated cyber attacks debilitated the Georgian government’s communication and response nodes.<sup>17</sup> After Georgian cyber systems were degraded, Russia physically invaded with its military.<sup>18</sup> Coordinated cyber attacks of the future will certainly be larger in scope and magnitude. The cyber attacks that preceded the Georgian invasion are a clarion call for what may come if America fails to mend the holes in its cyber defense.

Part II of this note details the current utilities critical infrastructure. Part III discusses the challenges Congress faces in establishing a comprehensive cyber

---

<sup>12</sup> See US-CERT, <http://www.us-cert.gov/about-us>.

<sup>13</sup> Nicole Perloth, *Luring Young Web Warriors Is a U.S. Priority. It’s Also a Game*, N.Y. TIMES, Mar. 24, 2013, <http://www.nytimes.com/2013/03/25/technology/united-states-wants-to-attract-hackers-to-public-sector.html>.

<sup>14</sup> See ICS-CERT, <http://www.us-cert.gov> (last visited Aug. 1, 2013).

<sup>15</sup> See FAR 52.241-6 (1995), *available at* <https://www.acquisition.gov/far/reissue/FARvol2ForPaperOnly.pdf>.

<sup>16</sup> Anne Barnard, *Georgia and Russia Nearing All-Out War*, N.Y. TIMES, Aug. 9, 2008, <http://www.nytimes.com/2008/08/10/world/europe/10georgia.html>.

<sup>17</sup> Jaak Aviksoo, Minister of Def. of the Republic of Estonia, Address at the Center for Strategic and International Studies: Cyberspace a New Dimension at our Fingertips (Nov. 28, 2007), *available at* [http://csis.org/files/media/csis/events/071128\\_estonia.pdf](http://csis.org/files/media/csis/events/071128_estonia.pdf).

<sup>18</sup> *Id.*

defense. Part IV explores patchwork solutions that administrative agencies have implemented in an effort to mitigate cyber attacks in utilities. Part V discusses how administrative agencies can leverage the existing government-contract framework to establish minimum cyber security requirements for utilities companies. Part VI illustrates the consequences for failing to establish a coherent cyber defense, using the Russian attack on Georgia as a case study.

## II. UTILITIES CRITICAL INFRASTRUCTURE

### A. *Increased Attacks*

The nation's critical infrastructure is vulnerable to cyber attack and must be protected. In recent years, critical infrastructure has increased productivity and efficiency by relying on cyberspace network control systems.<sup>19</sup> Critical infrastructures are the systems, networks, and assets so vital to the nation that their incapacitation or destruction would severely degrade the country's ability to function.<sup>20</sup> Critical infrastructures are primarily the financial, energy<sup>21</sup>, and emergency services sectors.<sup>22</sup> Critical infrastructures rely on control nodes to leverage cyberspace to increase productivity and efficiency. Cyberspace is comprised of hundreds of thousands of computers, servers, and control nodes connected by fiber optic cables.<sup>23</sup> Cyber attacks have dramatically increased over the past decade.<sup>24</sup> Attacker capacity is a legitimate threat to national security. Individual groups as well as other countries are attacking utilities control nodes.<sup>25</sup> Those entities are bypassing the U.S.'s traditional land, sea, and air defenses by exploiting cyber vulnerabilities.<sup>26</sup> Utilities critical infrastructure will continue to be attacked until cyber security improves.

### B. *Market Insulation*

Utilities are insulated from the socioeconomic pressures that affect businesses in other sectors. The financial critical infrastructure sector for example, is highly sensitive to socioeconomic pressures. Cyber attacks on the financial sector erode consumer confidence, halt markets, and expose

---

<sup>19</sup> Napolitano, *supra* note 2.

<sup>20</sup> Critical Infrastructure Protections Act of 2001, §1016 42 U.S.C. §5195c (2001).

<sup>21</sup> In this note the energy sector is referred to as the utilities sector.

<sup>22</sup> 42 U.S.C. §5195c.

<sup>23</sup> US-CERT, THE NAT'L STRATEGY TO SECURE CYBERSPACE 1, *available at* [http://www.us-cert.gov/reading\\_room/cyberspace\\_strategy.pdf](http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf).

<sup>24</sup> *Id.* at 6.

<sup>25</sup> Siobhan Gorman, *Alert on Hacker Power Play: U.S. Official Signals Growing Concern Over Anonymous Group's Capabilities*, WALL ST. JOURNAL, Feb. 21, 2012, <http://online.wsj.com/article/SB10001424052970204059804577229390105521090.html>.

<sup>26</sup> Tzu, *supra* note 1, at 62.



confidential consumer information.<sup>27</sup> When consumers discover that banks have lost control of their information or assets, they demand better protections. If additional protections are not provided, consumers take their business elsewhere. Socioeconomic pressures incentivize the financial sector to proactively respond to cyber related threats. Utilities are not as responsive to market pressures in part because of their legal history.

Historically, courts have validated government-subsidized monopolies in the utilities sector.<sup>28</sup> Courts generally have held that these monopoly arrangements are legitimate government pursuits and in accord with the Commerce Clause.<sup>29</sup> Unlike in the financial sector, changing regional utility providers can be a bit more challenging, if not impossible. In addition, utility companies are at times not held liable for damages caused from their services.<sup>30</sup> While the government may be liable for damages caused by negligence<sup>31</sup>, state law governs whether there are grounds to bring the claim.<sup>32</sup> Utilities claims are filed pursuant to the choice of law rules where the alleged act occurred.<sup>33</sup> This legal framework provides little incentive for filing claims for damages against utilities. With limited exposure to legal recourse from consumers for damages, utilities are inadequately incentivized to increase cyber security. As a result, utilities are exposed to the threat of cyber attacks without an adequate defense.

Although helpful, self-preservation prompted by socioeconomic pressures is not the solution. The free market approach yields an unreliable patchwork defense. For example, in 2010, hackers launched a denial-of-service attack ("DoS attack") on the NASDAQ website creating a temporarily jolting disruption

---

<sup>27</sup> Jenny B. Davis, *Cybercrime Fighters: Companies Have More Legal Weapons to Defend Against Attacks on Their Computer Systems*, 89 A.B.A. J., Aug. 2003, at 36.

<sup>28</sup> GMC, 519 U.S. at 289-90. (1997), *see also* Panhandle Eastern Pipe Line Co., 341 U.S. at 333.

<sup>29</sup> *Huron Portland Cement Co. v. Detroit*, 362 U.S. 440, 443-44 (1960) (stating that state actions that indirectly affect commerce do not prohibit states from legislating on the health, life, and safety of their citizens, though the legislation might indirectly affect commerce), *see also* *Gibbons v. Ogden*, 22 U.S. at 1, 21 (1824) (stating that States can enact legislation that creates monopolies and regulate commerce for the advantage of the community so long as it does not encroach on ground constitutionally reserved for the exclusive control of Congress.), *see, e.g.*, *Hall v. De Cuir*, 95 U.S. 485, 488 (1878) (stating that state legislation that regulates commerce within the state but does not seek to influence interstate commerce does not violate interstate commerce).

<sup>30</sup> *Maxim Integrated Prods. v. United States*, 1988 Cal. Unrep., \*1, \*18 (N.D. Cal. Dec. 4, 1998).

<sup>31</sup> 28 U.S.C. § 1346(b)(1), *see also* *United States v. Muniz*, 374 U.S. 150, 153 (1963) (stating that a claim against the government can be made where a private person under like circumstances would be liable under state law).

<sup>32</sup> *United Scottish Ins. Co. v. United States*, 614 F.2d 188, 195-96 (9th Cir. 1979).

<sup>33</sup> 28 U.S.C. §1346(b)(1); *see also* *Richards*, 369 U.S. at 10.

of the market.<sup>34</sup> DoS attacks seek to make cyber systems inaccessible by engaging them for prolonged periods of time from thousands of individual computers.<sup>35</sup> In 2011, the hacker group "Anonymous" attempted to "erase" the NYSE webpage as a gesture of support for the Occupy Wall Street protests.<sup>36</sup> These examples illustrate the limitations of relying solely on socioeconomic pressures as a defense to cyber attacks. Yet, as thin as the layer of cyber security in the financial sector is, it is virtually non-existent in the utilities sector.

### C. Calls for Action

The chorus of U.S. officials warning about utilities vulnerabilities is growing. Within the various echelons of the U.S. government, agency leaders are voicing their concerns about cyber attacks. Former Secretary of Defense Leon E. Panetta compared the current cyber threat to Pearl Harbor.<sup>37</sup> The Secretary's World War II analogy warns of a large-scale surprise attack on several critical infrastructures. The result of that attack would be a massive disruption of services and loss of life.<sup>38</sup> According to Panetta, hackers have already infiltrated electricity and water plant cyber control systems.<sup>39</sup> Echoing Panetta, Secretary of State John Kerry, during his Senate confirmation hearings, warned the Senate Foreign Relations Committee of the dangers cyber attacks pose to the nation's energy sector.<sup>40</sup> Secretary of the Department of Homeland Security Janet Napolitano characterized utilities attacks as setting up a potential "cyber 9/11."<sup>41</sup> In the absence of legislative solutions, these agency heads are implementing stopgap measures to combat cyber threats.

---

<sup>34</sup> Michael J. McFarlin, *NASDAQ, CBOE, Bats Hit by Cyber-Attacks*, THE FUTURES MAGAZINE, Feb. 15, 2012, <http://www.futuresmag.com/News/2012/2/Pages/Bats-CBOE-Nasdaq-hit-by-cyberattack.aspx>.

<sup>35</sup> John Markoff, *Georgia Takes a Beating in the Cyberwar With Russia*, N.Y. TIMES, Aug. 11, 2008, <http://bits.blogs.nytimes.com/2008/08/11/georgia-takes-a-beating-in-the-cyberwar-with-russia/>.

<sup>36</sup> *Id.*

<sup>37</sup> Panetta, *supra* note 9.

<sup>38</sup> Elizabeth Bumiller, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, N.Y. TIMES, Oct. 11, 2012, <http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html>.

<sup>39</sup> *Id.*

<sup>40</sup> Gerry Smith, *John Kerry: Foreign Hackers Are '21st Century Nuclear Weapons'*, HUFFINGTON POST, Jan. 24, 2013, [http://www.huffingtonpost.com/2013/01/24/john-kerry-hackers\\_n\\_2544534.html](http://www.huffingtonpost.com/2013/01/24/john-kerry-hackers_n_2544534.html).

<sup>41</sup> Jim Finkle, *Cyber 9/11 could happen 'imminently,' says US Homeland Security chief*, REUTERS, Jan. 24, 2013, <http://www.nbcnews.com/technology/technolog/cyber-9-11-could-happen-imminently-says-us-homeland-security-1C8103556>.

### III. THE ROLE OF CONGRESS IN FINDING A SOLUTION

#### A. *Cyber Security Legislation*

Congress must find a way to pass comprehensive cyber security legislation. Congress is the only governmental body capable of creating a comprehensive cyber security plan.<sup>42</sup> Cyber security legislation has steadily gained support for securing critical infrastructure since the year 2000.<sup>43</sup>

One of the most comprehensive cyber-security bills was the Cyber Security Enhancement Act of 2012 (“CSA2012”).<sup>44</sup> The bill never made it out of committee however, failing to acquire the 60 votes needed for a Senate general member vote.<sup>45</sup> CSA2012 attempted to tackle two of Congress’ biggest challenges: (1) maintaining civil liberties, and (2) ensuring public safety. The bill addressed civil liberties in Section 204 through the promotion of public awareness and education about current cyber threats.<sup>46</sup> The section called for efforts to make cyber security best practices known and usable to all public businesses.<sup>47</sup> The effort was strengthened by a late amendment that specifically allowed the government to share threat information with private industries controlling critical infrastructure.<sup>48</sup> These were much-needed steps in the right direction.

#### B. *Providing for Security*

The public must be informed of the threats cyber attacks pose to national security. Section 203 of the bill addressed the security technical standards for providing adequate security to critical infrastructure.<sup>49</sup> Specifically, Section 203 called for the accelerated development of interoperable security standards to secure interoperability between the government and private businesses.<sup>50</sup> The section also called for security frameworks that complied with privacy

---

<sup>42</sup> Napolitano, *supra* note 2.

<sup>43</sup> Cyber Security Information Act of 2000, H.R. 4246, 106th Cong., §§2-6 (2000).

<sup>44</sup> Cybersecurity Enhancement Act of 2012, H.R.2096, 112th Cong., §§101-06 (2011).

<sup>45</sup> Michael Schmidt, *Cybersecurity Bill Is Blocked in Senate by G.O.P. Filibuster*, N.Y. TIMES, Aug. 2, 2012, <http://www.nytimes.com/2012/08/03/us/politics/cybersecurity-bill-blocked-by-gop-filibuster.html>.

<sup>46</sup> H.R. 2096, 112th Cong. (2012).

<sup>47</sup> *Id.*

<sup>48</sup> Cyber Intelligence Sharing and Protection Act of 2012, *amended by* H.R. 3523, 113th Cong. (2012) (amending CISPA to make explicit that nothing in the legislation would prohibit a department or agency of the federal government from providing cyber threat information to owners and operators of critical infrastructure).

<sup>49</sup> *Id.*

<sup>50</sup> *Id.*

requirements.<sup>51</sup> This was an effort to ensure a firm line between public and private cooperation would be observed. Interoperability, collaboration, and privacy assurance are essential to creating a coherent cyber defense network that spans government and private business systems.

### *C. Cyber Security Legislation in 2013*

The Cyber Security and American Cyber Competitiveness Act of 2013 ("S.21") was introduced to the Senate and referred to the Committee on Homeland Security and Government Affairs.<sup>52</sup> S.21 sets a broad set of criteria in order to gain consensus. Specifically, it seeks to create a framework for developing public-private systems that protect critical infrastructure, such as utilities.<sup>53</sup> A focal point of S.21 is the attempt to find the balance between civil liberties and public safety that CSA2012 could not.<sup>54</sup> Although the bill is in its initial stages, Congress should incorporate the sections 203 and 204 of CSA2012. Those sections should be foundational components of the legislation because they contain innovative proposals for public safety and the protection of civil liberties.

### *D. The Fourth Amendment*

The legislative solution must be congruent with the spirit and the letter of the Fourth Amendment of the U.S. Constitution. The Fourth Amendment affords U.S. citizens the right to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.<sup>55</sup> In order to prevent warrantless monitoring, the Fourth Amendment must govern any proposal for government access to private utilities networks.<sup>56</sup> Yet, some government officials have proposed unilateral executive action. Notably, Secretary Panetta stated that, although there is no substitute for legislation, the Obama administration is working on an executive order on cyber security.<sup>57</sup> Although Panetta's appeals to urgency may be well founded, government intrusion into private businesses is not a solution.

---

<sup>51</sup> *Id.*

<sup>52</sup> LIBRARY OF CONG., BILL SUMMARY AND STATUS H.R. 3523, 113TH CONG. (May 7, 2012), <http://thomas.loc.gov/>.

<sup>53</sup> *Id.*

<sup>54</sup> *Id.*

<sup>55</sup> U.S. CONST. amend. IV.

<sup>56</sup> Lolita Baldor, *U.S. Cybersecurity Efforts Trigger Privacy Concerns*, WASH. TIMES, Jan. 27, 2012, <http://www.washingtontimes.com/news/2012/jan/27/cybersecurity-efforts-trigger-privacy-concerns>.

<sup>57</sup> Nicholas Hoover, *DOD: Hackers Breached U.S. Critical Infrastructure Control Systems*, INFO. WEEK, Oct. 12, 2012, <http://www.informationweek.com/government/security/dod-hackers-breached-us-critical-infrast/240008972>.

The U.S. government cannot handle this threat alone. Government intrusions into homes and businesses will not create secure cyber networks. The interdependent relationship between government and critical infrastructure companies relies on each party accessing cyberspace to secure the space that they own, or operate in.<sup>58</sup> Director of the National Security Agency General Keith Alexander noted that complex problems posed by cyber attacks do not require sacrificing civil liberties for security.<sup>59</sup> Establishing a common ground between security and civil liberties should be a starting point in establishing a comprehensive cyber defense.

### *E. Learning from Past Failures*

The role of technology in the debate between civil liberties and public safety is not new. In the 1928 case *Olmstead v. United States*, the Supreme Court debated whether the advantages gained over certain criminal activity warranted narrowing the Fourth Amendment of all citizens.<sup>60</sup> There, the Court held that the use of evidence from private telephone conversations intercepted by wire-tapping was not a violation of the Fourth Amendment because the threat outweighed the need for civil liberties.<sup>61</sup> There, the Supreme Court prescribed an unimaginatively rigid solution that resulted in legal government wiretapping. The United States cannot afford repeat the mistakes made in cases like *Olmstead*. As in Sections 203 and 204 of CSA2012, the government must promote solutions that conform to the Fourth Amendment while ensuring adequate cyber security.<sup>62</sup> Handwringing is not a plan. Although vigilance is tempered by the knowledge that the greatest threats to freedom come in times of crisis,<sup>63</sup> the U.S. government cannot give in to the stagnating principle of paralysis by analysis.

---

<sup>58</sup> THE NAT'L STRATEGY TO SECURE CYBERSPACE, *supra* note 21, at 11.

<sup>59</sup> James Ryan, *NSA Director on Cyberattacks: 'Everybody's Getting Hit'*, ABC NEWS, Nov. 7, 2012, <http://abcnews.go.com/blogs/politics/2012/11/nsa-director-on-cyberattacks-everybodys-getting-hit/>.

<sup>60</sup> *Olmstead v. United States*, 227 U.S. 438 (1928) *overruled by* *Katz v. United States*, 389 U.S. 347 (1967) (holding that Court's immaterial intrusions using technology as a search can constitute an unreasonable search and seizure pursuant to the Fourth Amendment and expanded its reach to provide protection to all areas a person has a reasonable expectation of privacy).

<sup>61</sup> *Id.*

<sup>62</sup> See H.R. 2096, 112th Cong. (2011).

<sup>63</sup> *Vernonia School Dist. 47J v. Action*, 515 U.S. 646 (1995) (Justice O'Connor dissenting, stating that student athletes' expectation of privacy outweighs public hysteria and demands for public safety).

### *F. Public-Private Partnership is Essential*

The government must work with, rather than act upon privately owned utilities. There is an interdependent relationship between utilities critical infrastructures and the private companies that own and operate them.<sup>64</sup> The balance in the public-private relationship would be shattered if an *Olmstead* approach prevailed. Government officials that push for coercive measures should be mindful not to alienate private businesses. Congress must continue to work on creating a solution that fosters public-private cooperation. The government must strive to work with private utility companies on common grounds. The largest of which is the protection of private assets that directly impact the lives of many citizens.

The government seems to understand its burden in creating an amicable environment for information sharing. The government's approach to the Einstein 3 program is an example of how it can inform and build public confidence in cyber security. Einstein 3 is a government network monitoring system that detects and reacts to cyber attacks on federal systems.<sup>65</sup> DHS officials have encouraged an open dialogue about the program in an effort to illustrate the extensive privacy protections already in place.<sup>66</sup> Such is a much needed gesture on behalf of the government to build public "trust and strict confidentiality" in the program.<sup>67</sup> An environment where the government and private companies freely exchange cyber threat information is a superior model to that of government monitoring. The goal of information sharing should be to create a seamlessly integrated cyber defense that blocks or blunts attacks. As cyber attacks continue to grow in intensity and frequency, the consequences of failure become more severe.

### *G. Avoiding Reactionary Measures*

Congress has an opportunity to balance security and civil liberties while the threat is still manageable. Other countries have avoided the issue and are now taking drastic measures to address cyber threats. Australia and Great Britain, for example, are forcing private companies to invest resources in cyber defense and share internal data about attacks.<sup>68</sup> In Great Britain, cyber attacks are now regarded as a top threat to national security.<sup>69</sup> Those drastic measures were

---

<sup>64</sup> THE NAT'L STRATEGY TO SECURE CYBERSPACE, *supra* note 21, at 2.

<sup>65</sup> Baldor, *supra* note 50.

<sup>66</sup> *Id.*

<sup>67</sup> *Id.*

<sup>68</sup> Gillian Tett, *Time to Break Wall of Silence on Escalating Cyber Attacks*, FIN. TIMES, Jan. 25, 2013, <https://www.fidelity.co.uk/investor/news-insights/expert-opinions/details.page?whereParameter=gillian-tett/escalating-cyber-attacks>.

<sup>69</sup> Francis Maude, Member of British Parliament, Address at the International Center for

taken because the privately owned critical infrastructure sectors failed to maintain inadequate cyber security.<sup>70</sup> Congress can avoid resorting to draconian measures by promoting information sharing and establishing minimum cyber security standards in legislation.<sup>71</sup> Congress can only pass legislation by working on common ground to shore up the weak links in the cyber defense chain.

#### IV. PATCHWORK SOLUTIONS

##### A. Administrative Agency Solutions

In the wake of persistent attacks, administrative agencies are creating patchwork cyber solutions. Administrative agencies are semi-autonomous government bodies that execute legislative, judicial, or executive functions.<sup>72</sup> The apolitical nature of administrative agencies enables them to create solutions to large problems while withstanding political pressure.<sup>73</sup> One agency that has been particularly active in establishing cyber security measures is the Department of Homeland Security. Congress established DHS as one of the fifteen administrative agencies of the executive branch.<sup>74</sup> It is responsible for preventing and minimizing terrorist attacks on the U.S.<sup>75</sup> The Department's attempts to tackle cyber security problems provide examples of how administrative agencies can provide intermediate solutions to politically complex problems.

##### B. The Department of Homeland Security

###### i. Recruiting Future Cyber Warriors

DHS has established several programs to combat cyber threats. One program focuses on recruiting future cyber security specialists on college campuses. At San Jose State University, for example, Secretary Napolitano laid out a plan to build a cyber security workforce to combat cyber attacks in an address to students.<sup>76</sup> At George Mason University, DHS created a cyber

---

Defense Studies in Estonia (May 3, 2012), *available at* <https://www.gov.uk/government/speeches/francis-maude-speech-at-the-international-centre-for-defence-studies-icds-in-Estonia>.

<sup>70</sup> *Id.*

<sup>71</sup> Napolitano, *supra* note 2.

<sup>72</sup> Peter L. Strauss, *The Place of Agencies in the Government: Separation of Powers and the Fourth Branch of Government*, 84 COLUM. L. REV. 573, 583-84 (1984) (identifying modern functions of administrative agencies).

<sup>73</sup> *Id.* at 586.

<sup>74</sup> Executive Departments, 5 U.S.C. § 101 (2013).

<sup>75</sup> Homeland Security Act of 2002, P.L. 107-296, 107th Cong. (2002).

<sup>76</sup> Napolitano, *supra* note 2.

specialist recruiting competition called the “Virginia Governor’s Cup Cyber Challenge.”<sup>77</sup> The competition was modeled on a program implemented by the Chinese government.<sup>78</sup> The government must continue these recruiting programs to prepare for future threats. In addition to preparing for future threats, DHS established programs to deal with current threats.

ii. Addressing Current Threats to Utilities

DHS programs rely on overt government monitoring and self-reporting. The U.S. Computer Emergency Readiness Team (“US-CERT”) is a watch and warning center that responds to cyber security threats to infrastructure systems.<sup>79</sup> It is a system that detects attacks after they have occurred. The focus of US-CERT is rapid response and damage mitigation. The program enables the government to repair infrastructure cyber systems soon after they are detected. In its current application, US-CERT is a completely reactionary program. Conversely, the Industrial Control Systems Cyber Emergency Response Team (“ICS-CERT”) attempts to reduce threats to utilities based on self-reporting.<sup>80</sup> It partners intelligence and law enforcement agencies with private utilities to collaborate and share cyber threat information.<sup>81</sup> The program provides private utilities an opportunity to interface with government agencies about the vulnerabilities of their cyber control nodes before a debilitating attack.<sup>82</sup> This forward-thinking program captures the tone the legislature should seek to replicate in legislation.

ICS-CERT fosters the public-private relationship between utilities and government agencies. It also functions as an on-call incident response team that provides situational awareness and triages cyber attacks on critical infrastructure.<sup>83</sup> In 2010, the first full year of ICS-CERT, DHS recorded 41 reported attacks on utilities.<sup>84</sup> In the year 2011 the number rose to 198.<sup>85</sup> All reported attacks were conducted through cyberspace using methods ranging from spear phishing to website hyperlinks.<sup>86</sup> The main drawback to this

---

<sup>77</sup> Nicole Perloth, *Luring Young Web Warriors Is a U.S. Priority. It’s Also a Game*, N.Y. TIMES, Mar. 24, 2013, <http://www.nytimes.com/2013/03/25/technology/united-states-wants-to-attract-hackers-to-public-sector.html>.

<sup>78</sup> *Id.*

<sup>79</sup> US-CERT, *supra* note 9.

<sup>80</sup> Critical Infrastructure Sec. and Resilience, Presidential Policy Directive 21 (2013).

<sup>81</sup> *Id.*

<sup>82</sup> ICS-CERT, *supra* note 11.

<sup>83</sup> U.S. DEP’T OF HOMELAND SECURITY, ICS-CERT INCIDENT RESPONSE SUMMARY REPORT 2009-2011 17, <http://ics-cert.us-cert.gov/sites/default/files/ICS-CERT%20Incident%20Response%20Summary%20Report%20%282009-2011%29.pdf>.

<sup>84</sup> *Id.* at 5.

<sup>85</sup> *Id.*

<sup>86</sup> *Id.* at 13.



program, however, is that it relies on volunteer reporting from companies that have little incentive to participate. This self-reporting method, although helpful, is only a fraction of what is required to combat cyber threats.

### iii. Severity of the Threat

Unreported cyber threats can lead to debilitating consequences. In August 2003, an unreported Internet computer worm corrupted the control systems of Ohio's Davis-Besse Nuclear Power Plant.<sup>87</sup> The attack left thousands without power four hours. Similarly, an attack on utility control systems that manage dams could cause an overflow, which would devastate a local area.<sup>88</sup> A coordinated attack on multiple power plants would result in massive catastrophe and would lead to the displacement of countless Americans.<sup>89</sup> Of additional concern is the fact that the federal government and the Department of Defense purchase over 29 million megawatt-hours of electricity annually.<sup>90</sup> A well-coordinated attack on utilities could significantly impact the government's ability to function.

Utilities are the most targeted of all critical infrastructure sectors. While the exact number of attacks on utilities is unknown, it is clear that attacks are increasing. Approximately 60% of all cyber attacks on critical infrastructures in the year 2011 were on utilities.<sup>91</sup> In the year 2012, ICS-CERT estimated approximately 7,200 utility control system devices were targeted by advanced persistent threat activity.<sup>92</sup> Analysis of these trends highlights both the gaunt state of the U.S.'s utility cyber security and the opportunistic nature of cyber attackers. It is sobering to note that those reports only reflect reported attacks. Despite the efforts of DHS to work with private businesses, there is no way to tell how many cyber attacks go unreported. The U.S.'s critical infrastructure should not depend on private companies volunteering information. Congress must enact comprehensive legislation that provides a baseline cyber security defense.

<sup>87</sup> Kevin Poulsen, *Slammer Worm Crashed Ohio Nuke Plant Network*, SEC. FOCUS, Aug. 19, 2003, <http://www.securityfocus.com/news/6767>.

<sup>88</sup> Natasha Solce, *The Battlefield Of Cyberspace: The Inevitable New Military Branch - The Cyber Force*, 18 Alb. L.J. Sci. & Tech. 293, 303 (2008).

<sup>89</sup> Napolitano, *supra* note 2.

<sup>90</sup> Anthony Andrews, *Federal Agency Authority to Contract for Electric Power and Renewable Energy Supply Study*, CONG. RESEARCH SERV. 1 (Aug. 15, 2011), <http://www.nationalaglawcenter.org/assets/crs/R41960.pdf>.

<sup>91</sup> ICS-CERT, *supra* note 75, at 5.

<sup>92</sup> U.S. DEP'T OF HOMELAND SECURITY, ICS-CERT MONITOR OCT./NOV./DEC. 2012 4-5, *available at* [http://ics-cert.us-cert.gov/sites/default/files/ICS-CERT\\_Monthly\\_Monitor\\_Oct-Dec2012\\_2.pdf](http://ics-cert.us-cert.gov/sites/default/files/ICS-CERT_Monthly_Monitor_Oct-Dec2012_2.pdf).

## V. CONTRACTING A STOPGAP FROM THE EXISTING UTILITIES FRAMEWORK

### A. *How Contracting Can be Effective*

Administrative agency contracting would provide a stopgap solution to the utilities cyber security problem. The government has the authority to enter into contracts with private utilities.<sup>93</sup> Contracting would affect utilities in a way that market pressures do not. Government contracting could nudge the utilities sector to change, update, or modernize their cyber security systems in order to stay in business. Through contracting, the federal agencies could require private utility companies to comply with minimum cyber security standards. Minimum standards could be used as the entry criteria for bidding and maintaining government contracts. This would increase the amount of utilities implementing adequate cyber security while creating a uniform line of defense.

### B. *Using Preexisting Contract Frameworks*

Although there is currently no minimum cyber security requirement for utilities contracts, the framework for physical security is well established. The government has the authority to regulate privately owned utilities in the interest of public safety.<sup>94</sup> Several examples include the Public Utilities Holding Company Act ("PUHCA"), the Federal Property Administration Act ("FPAA"), and Title 42 of the United States Code. PUHCA requires companies to report specific information to the government on the grounds of public safety.<sup>95</sup> FPAA is a Department of Energy ("DOE") regulation, which grants the General Services Administration the authority to establish methods and policies for acquiring utility services to federal agencies.<sup>96</sup> FPAA may be able to add cyber policy requirements at its discretion. Title 42 of the United States Code authorizes the DOE to initiate and modify energy contracts with private utilities companies.<sup>97</sup> Accordingly, the DOE may be able to incorporate cyber requirements into contracts as well.

---

<sup>93</sup> Department of Energy Acquisition Policy, 48 C.F.R. §41.103 (2013); *See also* Anthony, *supra* note 80, at 3.

<sup>94</sup> *See PG&E Corp. v. Public Utilities Com.*, 118 Cal. App. 4th 1174, 1184 (Cal. App. 1st Dist. 2004) (establishing that the Commission has the authority to impose and enforce actions pursuant to enforcement of the Public Utilities Act); *see also General Tel. Co. v. Public Utility Com.*, 628 S.W.2d 832, 839 (Tex. App. Austin 1982).

<sup>95</sup> *See* Joseph Woodle, Dir. Div. of Corp. Regulation SEC., Remarks at Conference on Securities Laws and Regulation (Feb. 19-20, 1959), <http://www.sec.gov/news/speech/1959/0219-2059woodle.pdf>; *see also PG&E Corp.*, Cal. App. 4th at 1184; *see also General Tel. Co.*, 638 S.W. 2d at 839.

<sup>96</sup> Fed. Prop. and Admin. Serv. Act of 1949, 40 U.S.C. § 201 (2000).

<sup>97</sup> 42 U.S.C. §7256 (2006).

## i. Two Potential Approaches

Between PUCHA and FPAA two potential contractual approaches emerge. In the first approach utilities would agree to government monitoring. The government would monitor internal business networks to ensure minimum cyber security requirements are maintained. Enacted in 1935, PUCHA was implemented to protect consumers from risky utility company practices.<sup>98</sup> It is one example of how administrative agencies could use contracts to increase cyber security by monitoring. In 2005, the reformed PUHCA maintained its oversight requirement to ensure utilities remain reliable and functional.<sup>99</sup> Additionally, the Act requires utilities holding companies to make their financial books, accounts, memoranda, and costs available for government review.<sup>100</sup> Accordingly, this framework may allow administrative agencies to require utilities to report expenses spent preventing or rebuilding after network attacks. Similarly to the present situation, at that time utilities companies leveraged the short-term benefits of risky behavior while exposing the population to unacceptable risks.<sup>101</sup> This utilities-focused regulation is an example for how administrative agencies can enhance cyber security through contracting.

PUHCA has the internal mechanics required to regulate and enforce cyber security through contracting. Specifically, Section 366.1 establishes the Federal Energy Regulation Commission ("FERC") as the administrative action for enforcing PUCHA.<sup>102</sup> FERC is an independent agency that regulates the interstate transmission of utilities.<sup>103</sup> FERC enforces regulatory requirements through the imposition of civil penalties and punishments.<sup>104</sup> Its mission is to promote the development of safe, reliable, and efficient utilities infrastructure that serves the public interest.<sup>105</sup> The purpose for requiring government access to sensitive information was for the protection of the populace. As a safeguard for preventing a company's sensitive internal information, Section 1264(d)

<sup>98</sup> See Remarks from Joseph Woodle, *supra* note 87, at 1.

<sup>99</sup> FED. ENERGY REGULATION COMM'N, FEDERAL ENERGY REGULATION FACT SHEET ENERGY POLICY ACT 2005 (2006), available at <http://www.ferc.gov/legal/fed-sta/epact-fact-sheet.pdf>.

<sup>100</sup> Energy Policy Act of 2005, Pub. L. No. 109-58, § 1275(b) 119 Stat. 594, 977 (2005); see also *Morgan Stanley Capital Grp., Inc. v. Pub. Util. Dist. No. 1 of Snohomish Cnty.*, 554 U.S. 527, 531, (2008) (holding that energy companies must file their rate schedules and service contracts).

<sup>101</sup> See Remarks from Joseph Woodle, *supra* note 87, at 1.

<sup>102</sup> Repeal of the Public Utility Holding Company Act of 1935 and Enactment of the Public Utility Holding Company Act of 2005, 18 C.F.R. § 335 (2005) (repealed 2005), available at <http://www.ferc.gov/whats-new/comm-meet/091505/M-1.pdf>.

<sup>103</sup> FERC, WHAT FERC DOES, <http://www.ferc.gov/about/ferc-does.asp> (last visited Aug. 1, 2013).

<sup>104</sup> *Id.*

<sup>105</sup> U.S. FED. ENERGY REGULATION COMM'N, THE STRATEGIC PLAN, FISCAL YEAR 2009-2014 3 (Revised 2013), available at <https://www.ferc.gov/about/strat-docs/FY-09-14-strat-plan-print.pdf>.

forbid any one with access to this information from disclosing it.

Required reporting and internal systems monitoring would aid established programs like ICS-CERT, but at too high a cost. The government would gain the benefit of not having to rely on volunteer information. Mandatory reporting may even increase government efficiency in preventing future attacks. One glaring drawback to this approach, however, is that it would put the solution squarely in the same position that Congress now finds itself in. This approach would all but certainly aggravate the ongoing civil liberties—public safety debate in Congress. Such an approach would likely frustrate the public-private relationship and create more problems than it would solve. A contract policy requiring private companies to allow government monitoring of internal cyber systems would likewise be doomed to failure.

In the second approach, administrative agencies merely verify that minimum cyber security standards are in place. This approach would consist of government verification of cyber security standards. DOE Federal Acquisition Regulation (“FAR”) requires all federal agency utilities contracts comply with its service provisions.<sup>106</sup> This less intrusive framework allows utilities to meet standards set and verified by the government through inspections.

FAR has the requisite structure to enforce a cyber capabilities inspection program. FAR, Section 52.241-6, specifies the physical requirements utilities must maintain to be in compliance with the contract.<sup>107</sup> While this area focuses on physical equipment, it could be expanded to address cyber security. This section calls for government participation in facility inspections to ensure utilities remain in compliance with the terms of the contract. This approach calls for reviewing utilities cyber security without invasive monitoring. Administrative agency inspections could have a significant impact on utilities.

This approach would give private utilities the freedom to choose how to meet the government’s standards. It would also avoid the ongoing civil liberties debate that has gridlocked Congress.

## VI. CONSEQUENCES OF FAILING TO ACT

### A. *Attacks in Perspective*

The consequences of failing to act would be disastrous. US-CERT has already responded to more than 106,000 incident reports of cyber attack to the critical infrastructure since the program began.<sup>108</sup> When viewed in a vacuum, one may be tempted to dismiss the national concern. Yet, when viewed as a trend, the

---

<sup>106</sup> FAR 52.241-6 (1995), *available at*

<https://www.acquisition.gov/far/reissue/FARvol2ForPaperOnly.pdf>.

<sup>107</sup> *Id.*

<sup>108</sup> Napolitano, *supra* note 2.

national significance arises to the foreground.

### B. *Cyber Attack on Georgia*

The cyber attack on the country of Georgia illustrates how cyber warfare will be used in future conflicts. In August 2008, Georgian forces launched an attack against separatist forces sympathetic to Russia.<sup>109</sup> Shortly thereafter, the Russian military invaded Georgia.<sup>110</sup> Before the Russian invasion, Georgia's governmental cyber systems were attacked.<sup>111</sup> The attack was broad and coordinated. The volume of Internet traffic into Georgia increased by 400 times during the attack.<sup>112</sup> The DoS attack disrupted the Georgian government's ability to function and respond to the Russian invasion. The cyber attacks on Georgia began weeks before it was physically invaded.<sup>113</sup> This was the first time a cyber attack immediately preceded a physical attack between two sovereign nations.<sup>114</sup> It will likely not be the last.

### C. *Cyber Attacks in the Future*

A fundamental tenet of warfare is deception.<sup>115</sup> The ability to leverage cyber attacks while remaining unidentified is a bellwether for future warfare.<sup>116</sup> Cyber attacks are relatively inexpensive, easy to execute, and the perpetrators rarely get caught.<sup>117</sup> As technology like the kind used in Georgia becomes more available, entities will continue to exploit cyber weaknesses in nations' critical infrastructures.<sup>118</sup> To this day the attacks on Georgia's cyber systems are

<sup>109</sup> See Anne Barnard, *Georgia and Russia Nearing All-Out War*, N.Y. TIMES, Aug. 9, 2008, <http://www.nytimes.com/2008/08/10/world/europe/10georgia.html>.

<sup>110</sup> *Senior Georgian Ministers Sacked*, BBC NEWS, (Dec. 5, 2008), <http://news.bbc.co.uk/2/hi/europe/7767799.stm>.

<sup>111</sup> *CNN American Morning: What Can the U.S. Do to Deal With the Russian Invasion of Georgia?* (CNN television broadcast Aug. 14, 2008, 7:47 AM) available at <https://advance.lexis.com/>.

<sup>112</sup> Jaak Aviksoo, Minister of Def. of the Republic of Estonia, Address at the Center for Strategic and International Studies: Cyberspace a New Dimension at our Fingertips (Nov. 28, 2007), available at [http://csis.org/files/media/csis/events/071128\\_estonia.pdf](http://csis.org/files/media/csis/events/071128_estonia.pdf).

<sup>113</sup> *The cyber raiders hitting Estonia*, BBC NEWS (May 17, 2007, 14:52 GMT), <http://news.bbc.co.uk/2/hi/europe/6665195.stm>.

<sup>114</sup> See Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED MAGAZINE, Aug. 21, 2007, available at [http://www.wired.com/politics/security/magazine/15-09/ff\\_estonia](http://www.wired.com/politics/security/magazine/15-09/ff_estonia).

<sup>115</sup> Tzu, *supra* note 1, at 42.

<sup>116</sup> William C. Ashmore, *Impact of Alleged Russian Cyber Attacks Impact of Alleged Russian Cyber Attacks*, SCHOOL OF ADVANCED MILITARY STUDIES, 12 (2008), available at <http://www.dtic.mil/dtic/tr/fulltext/u2/a504991.pdf>.

<sup>117</sup> John Markoff, *Before Gunfire, Cyber Attacks*, N.Y. TIMES, Aug. 12, 2008, <http://www.nytimes.com/2008/08/13/technology/13cyber.html>.

<sup>118</sup> Robert Gates, Sec'y of Def., Keynote Address at the Army War College (Apr. 16, 2009); see

unattributed.<sup>119</sup> With the successful attacks on Georgia firmly in mind, it is imperative that America solve its' cyber security issues.

## VII. CONCLUSION

America's critical infrastructure is vulnerable to cyber attacks. Threats and attacks to the U.S.'s utilities sector are not hypothetical—they are real and ongoing. The utilities sector is the most vulnerable critical infrastructure sector. They have come to rely on cyber controls to cut costs and increase efficiency. They have not however, reciprocally increased their cyber-security posture. Utilities have become the target of choice for cyber attackers. The public-private relationship between the government and utility companies has compounded the problem. Without market pressures, or the threat of suits for failures in service, utilities are lagging behind in cyber security. The stakes are too high to rely solely on individual companies to defend the nation's critical infrastructure. Only legislation passed by the U.S. Congress can provide comprehensive national defense to combat cyber threats.

Congress must find a workable solution to this complex problem. Central to the hotly contested cyber defense issue is the balance between civil liberties and public safety. The answer lies firmly in the confines of partnership between the government and private companies. Congress must foster an environment that promotes information sharing that reflects partnership. Resolving civil liberties issues has proven to be a daunting task; yet, while progress is being made cyber attacks continue to grow in frequency and magnitude.

Administrative agencies can immediately begin implementing stopgap cyber defense measures through contracting. The precedence, framework, and mechanics for utilities regulation pursuant to public safety are well established. Currently, agency contracts require specific and general physical security standards. However, they do not yet require a minimum cyber security threshold for acquiring or bidding on utility contracts. Contracting requirements allow the bidder to choose their own products and maintain their own systems. Although public-private information sharing and contracting is not a total solution, it would certainly help. Administrative agency contracting is an appropriate stopgap because it increases public safety without

---

also THE NAT'L STRATEGY TO SECURE CYBERSPACE, *supra* note 21, at 7; see also Jeanne Meserve, *Study Warns of Cyberwarfare During Military Conflicts*, CNN, Aug. 17, 2009, <http://www.cnn.com/2009/US/08/17/cyber.warfare/>.

<sup>119</sup> See Mark Rutherford, *Report: Russian Mob Aided Cyberattacks on Georgia*, CNET NEWS, Aug. 18, 2009, [http://news.cnet.com/8301-13639\\_3-10312708-42.html](http://news.cnet.com/8301-13639_3-10312708-42.html); see also Mike Collier, *Estonia: Cyber Superpower*, BLOOMBERG BUSINESS WEEK, December 17, 2007, <http://www.businessweek.com/stories/2007-12-17/estonia-cyber-superpowerbusinessweek-business-news-stock-market-and-financial-advice>.

encroaching on civil liberties. This stopgap would give the Congress breathing room to find an appropriate solution.

The consequences for failure to act are glaring. The cyber attack that preceded the invasion of Georgia was a clarion call for all nation-states. An attack on the United States will likely not come in the form of smoldering ships in the nation's seaports, or planes crashing into buildings—it will be with the anonymous click of a mouse that turns off our power grids, releases flood waters of dams, and melts down nuclear reactors.

America must continue pressing on towards a coherent solution with the understanding that civil liberties and national defense are not mutually exclusive of one another. Yet, as this debate continues, threats to the U.S.'s infrastructure become more sophisticated and effective. Only a comprehensive solution is capable of mending the gaping holes in the nation's common cyber defense.



**STUDENT NOTE**

**The Application of the Administrative Procedure Act to Private-Public Sector Partnerships in Homeland Security**

*Michael James Weiss* \*

ABSTRACT

*Increasingly, the U.S. federal government is turning to the use of private-public sector partnerships (“PPP”), especially in the area of homeland security. Although these partnerships have numerous benefits, there are several problems that arise in their practice, particularly when they are used in homeland security.*

*This note will outline and detail these problems, including deputization, excessive congressional oversight, and management and accountability. In addition, this note will present solutions to resolving the issue of centralization. In other words, this note will advocate for a single agency that implements, manages, and creates rules for all PPPs within the Department of Homeland Security. Finally, this note will argue that not only is there a need for this one managing agency, but that the agency should be governed under the principals of the Administrative Procedure Act (“APA”).*

Table of Contents

---

I. INTRODUCTION.....	173
A. <i>What is a Private-Public Sector Partnership?</i> .....	173
B. <i>How are Private-Public Sector Partnerships Used?</i> .....	174
i. Private-Public Sector Partnerships in Homeland Security.....	174
C. <i>Diagnosing the Problem</i> .....	175
i. Deputization.....	175
ii. Excessive Congressional Oversight.....	176
iii. Management and Accountability.....	176
D. <i>Solutions</i> .....	177
II. ISSUES IN APA IMPLEMENTATION.....	177

---

\* University of Miami School of Law, Class of 2014; Master’s in Public Administration, Class of 2014. The author would like to thank Professor Charlton Copeland for his assistance, editing, and guidance on this article. He would also like to thank Kaitlin L. O. Niccum for her love and support, as well as his family Harold, Lilyan, Richard, Jaclyn, Daniel, and Gregory for their love and guidance.



A. <i>Deputization</i> .....	177
B. <i>Excessive Congressional Oversight</i> .....	181
C. <i>Management and Accountability</i> .....	183
III. SOLUTIONS.....	184
A. <i>Overview</i> .....	184
B. <i>Deputization</i> .....	187
C. <i>Excessive Congressional Oversight</i> .....	189
D. <i>Management and Accountability Problems</i> .....	190
IV. BENEFITS OF APA IMPLEMENTATION.....	192
V. CONCLUSION.....	194

I. INTRODUCTION

A. *What is a Private-Public Sector Partnership?*

A private-public sector partnership (“PPP”) is “a contractual agreement between a public agency (federal, state, or local) and a private sector entity.”<sup>1</sup> In such partnerships, the assets of each party, both public and private are maximized for the public good.<sup>2</sup> The maximization occurs because these partnerships take the best features and attributes from both the private and public sectors in order to solve a single goal, or goals, in the most efficient manner.<sup>3</sup>

What separates PPPs from general government contracting with the private sector is that they provide more oversight of government officials.<sup>4</sup> In a PPP, there are better public managers that are more “attuned to communication with accountability oriented . . . metrics, goals, and expectations.”<sup>5</sup> These officials are more “attuned” with communication accountability “language” which calls for specific performance of goals, expectations, and metrics.<sup>6</sup> In other words, the government partners in a PPP are more involved in the process of the planning and implementation of

<sup>1</sup> THE NATIONAL COUNCIL FOR PUBLIC-PRIVATE PARTNERSHIPS, <http://www.ncppp.org/ppp-basics/7-keys/> (last visited Mar. 5, 2013) [hereinafter NCPPP]; see also Thomas A. Cellucci, *Innovative Public Private Partnerships: A Pathway to Effectively Solving Problems*, U.S. DEPARTMENT OF HOMELAND SECURITY, SCIENCE AND TECHNOLOGY DIRECTORATE, 4 (2011), available at [http://www.dhs.gov/xlibrary/assets/st\\_innovative\\_public\\_private\\_partnerships\\_0710\\_version\\_2.pdf](http://www.dhs.gov/xlibrary/assets/st_innovative_public_private_partnerships_0710_version_2.pdf).

<sup>2</sup> *Id.*

<sup>3</sup> *Id.*

<sup>4</sup> PAUL R. VERKUIL, *OUTSOURCING SOVEREIGNTY: WHY PRIVATIZATION OF GOVERNMENT FUNCTIONS THREATENS DEMOCRACY AND WHAT WE CAN DO ABOUT IT* 172 (2007).

<sup>5</sup> *Id.*

<sup>6</sup> Russell D. Howard, *Homeland Security and the New Terrorism*, HOMELAND SECURITY AND TERRORISM: READINGS AND INTERPRETATIONS 172 (2006).

programs.<sup>7</sup> Further, the relationship between the public and private partners is cooperative, where the government is involved in the process<sup>8</sup>, rather than in a typical contracting relationship where the private company is subordinate to the public, government partners.<sup>9</sup>

The U.S. federal government uses these “agreements” and partnerships to “gain” advantages prevalent in the private sector, without all of the drawbacks.<sup>10</sup> These advantages could include specialized expertise or skill sets<sup>11</sup>, better productivity<sup>12</sup>, and more resources.<sup>13</sup> Neither the private nor the public sectors have all the answers, but by combining the two sectors together, more information, and funding, is available.<sup>14</sup>

### B. *How Are Private-Public Sector Partnerships Used?*

The use of PPPs throughout the federal government is extensive. PPPs range from former Secretary of State Colin Powell's Global Development Alliance with private charities<sup>15</sup>, to the cleanup of the Rocky Flats Nuclear Weapons Production Plant with the help of Kaiser-Hill, a private company.<sup>16</sup> PPPs are used not only used in time of limited economic resources<sup>17</sup>, but when either a private or a public entity wants access to the other's resources. These resources are not limited to capital<sup>18</sup>, but can include expertise, information, or even greater efficiency.<sup>19</sup> Hence, PPPs are a win-win for all parties involved.

#### i. Private-Public Sector Partnerships in Homeland Security

It is evident that PPPs are used throughout the federal government and public sector in every imaginable way. This note will focus specifically on the PPPs that exist and should exist in the Department of Homeland Security (“DHS”). The DHS is specifically suited to the use of PPPs because homeland security is always evolving, shifting, and changing. Homeland security encompasses the prevention of cyber-attacks, the growth of international

---

<sup>7</sup> *Id.*

<sup>8</sup> *Id.*

<sup>9</sup> VERKUIL, *supra* note 4.

<sup>10</sup> JOHN D. DONAHUE & RICHARD J. ZECKHAUSER, COLLABORATIVE GOVERNANCE: PRIVATE ROLES FOR PUBLIC GOALS IN TURBULENT TIMES 27-32 (2011).

<sup>11</sup> *Id.* at 35.

<sup>12</sup> *Id.*

<sup>13</sup> *Id.* at 36.

<sup>14</sup> *Id.* at 35-36.

<sup>15</sup> *Id.* at 122-24 .

<sup>16</sup> *Id.* at 66-67.

<sup>17</sup> NCPPP, *supra* note 1.

<sup>18</sup> *Id.*

<sup>19</sup> *Id.*

terrorism, and even natural disasters, and this wide-ranging subject matter lends itself perfectly to alliances between the government and the private sector.<sup>20</sup>

While the areas that homeland security encompasses are growing, DHS's budget is currently \$59.9 billion for fiscal year 2014.<sup>21</sup> This may seem like an immense sum of money, but the reality is that this money must be stretched to cover some 240,000 employees and agents<sup>22</sup>, and the protective services for U.S. citizens and residents (and their property) in all 50 states and over 75 countries around the globe.<sup>23</sup> This budget provides very limited resources for such a wide range of responsibilities. One way to deal with the conflict between a lack of resources and the ever-growing and ever-changing list of threats<sup>24</sup> that face DHS, is to turn to private-public sector partnerships.<sup>25</sup> The use of private-public sector partnerships may be the only solution to allow DHS cover the wide breadth of its duties and goals within its limited budget.<sup>26</sup>

### C. Diagnosing the Problem

#### i. Deputization

Despite the numerous advantages of PPPs, they are not flawless. The first problem is deputization. Deputization is a government process in

---

<sup>20</sup> Quadrennial Homeland Security Review Report: A Strategic Report for a Secure Homeland, U.S. DEP'T OF HOMELAND SECURITY (Feb. 2010), *available at* [http://www.dhs.gov/xlibrary/assets/qhsr\\_report.pdf](http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf).

<sup>21</sup> U.S. DEP'T OF HOMELAND SECURITY, BUDGET-IN-BRIEF: FISCAL YEAR 2014, *available at* <http://www.dhs.gov/sites/default/files/publications/MGMT/FY%202014%20BIB%20-%20FINAL%20-508%20Formatted%20%284%29.pdf>.

<sup>22</sup> Rick Nelson and Rob Wise, *Homeland Security at a Crossroads: Evolving DHS to Meet the Next Generation of Threats*, CENTER FOR STRATEGIC AND INT'L STUDIES (Feb. 1, 2013), <http://csis.org/publication/homeland-security-crossroads-evolving-dhs-meet-next-generation-threats>.

<sup>23</sup> *Id.*

<sup>24</sup> National Security Preparedness Group, *Tenth Anniversary Report Card: The Status of the 9/11 Commission Recommendations*, THE BIPARTISAN POLICY CENTER, 16-17 (Sept. 2011), *available at* <http://bipartisanpolicy.org/library/report/tenth-anniversary-report-card-status-911-commission-recommendations>.

<sup>25</sup> James Jay Carafano, Jena Baker McNeill, and Paul Rosenzweig, *Stopping the Chaos: A Proposal for Reorganization of Congressional Oversight of the Department of Homeland Security*, HERITAGE FOUNDATION ISSUE BRIEF NO. 3046 (Nov. 4, 2010), *available at* <http://www.heritage.org/research/reports/2010/11/stopping-the-chaos-a-proposal-for-reorganization-of-congressional-oversight-of-dhs>.

<sup>26</sup> Thomas A. Cellucci, *Leveraging Public-Private Partnership Models and the Free Market System to Increase the Speed-of-Execution of High-Impact Solutions throughout State and Local Governments*, U.S. DEP'T OF HOMELAND SECURITY, 8 (Aug. 2011), *available at* <http://www.dhs.gov/xlibrary/assets/st-leveraging-partnerships-for-state-and-local-governments-August2011.pdf>.

homeland security where an individual or class of individuals assumes some or all of the official powers of a government agent.<sup>27</sup> In other words, a deputized agent acts in place of an actual government agent in the pursuit of government goals.<sup>28</sup> At its core, the idea of deputization is an excellent solution to a universe of limited resources, personal and material.<sup>29</sup> Deputization also allows government agents into places that they legally could not normally enter, such as private homes or offices.<sup>30</sup> However there is a major flaw in deputization, insofar as there is no oversight and accountability for the newly minted government agents.

ii. Excessive Congressional Oversight

The second major problem with PPPs is excessive congressional oversight.<sup>31</sup> Though some oversight is required legally and constitutionally mandated<sup>32</sup>, as DHS is an executive department<sup>33</sup>, oversight can still prove to be excessive. The problem of overreaching oversight is rooted in the multitude of committees that oversee the Department of Homeland Security.<sup>34</sup> The requirements that these committees place on DHS in terms of resources, time, personnel, and money spent on preparing for hearings and investigations is often excessive.<sup>35</sup> These activities are not only redundant, but they distract officials and staff from the true purpose of the DHS.<sup>36</sup>

iii. Management and Accountability

The final issue that will be discussed in this note is the improper management and accountability of PPPs in homeland security.<sup>37</sup> The current way PPPs are run in the Department of Homeland Security is scattered and disorganized.<sup>38</sup> There is no clear leadership or central authority to make these

---

<sup>27</sup> Jon D. Michaels, *Deputizing Homeland Security*, 88 TEX. L. REV. 1435, 1442. (2010).

<sup>28</sup> *Id.*

<sup>29</sup> *Id.* at 1438.

<sup>30</sup> *Id.*

<sup>31</sup> Carafano, *supra* note 25.

<sup>32</sup> U.S. CONST. amend. I, § 8.

<sup>33</sup> 50 U.S.C. § 1803.

<sup>34</sup> Michael L. Koempel, *Homeland Security: Compendium of Recommendations Relevant to House Committee Organization and Analysis of Considerations for the House, and 109th and 110th Congresses Epilogue*, CONG. RESEARCH SERV. (2007), available at <http://www.fas.org/sgp/crs/homsec/RL32711.pdf>.

<sup>35</sup> National Security Preparedness Group, *supra* note 24.

<sup>36</sup> *Id.*

<sup>37</sup> David W. Gaffey, *Outsourcing Infrastructure: Expanding the Use of Public-Private Partnerships in the United States*, 39 PUB. CONT. L.J. 351, 369 (2010).

<sup>38</sup> U.S. DEP'T OF HOMELAND SECURITY, DEPARTMENT-WIDE RESOURCES (last visited Mar. 5, 2013), <http://www.dhs.gov/sites/default/files/publications/Policy-PSO/psa-department-wide->

PPPs as efficient and effective as they can and should be.

#### D. *Solutions*

The solution to the problems presented in this note is to streamline and centralize the process of governing PPPs in DHS by bringing the myriad of programs and projects that utilize PPPs under one roof, governed by one central sub-agency of DHS. This program should be modeled after similar agencies already implemented in the United Kingdom and Canada, called Partnerships UK and Partnerships BC, respectively.<sup>39</sup> The details of these agencies, and how they provide a model for the governance of PPPs, will be discussed in Part II.

One element of including all PPPs under one roof is giving them a uniform code of regulation. This note proposes that the Administrative Procedure Act (“APA”) act as the uniform code of regulation under a new partnership agency. The APA is legislation that allows Congress to endow government agencies with the ability to make rules that carry the force of law.<sup>40</sup> Applying the APA will allow PPPs to be uniform in their governance, oversight, accountability, and transparency. The APA will take a collection of randomly charted, organized, and relatively unaccountable government programs, and will make them streamlined, able to be supervised properly, and efficient by governing under a uniform code of rules and laws.

Part II of this note will describe the previously mentioned problems of deputization, excessive congressional oversight, and management and oversight. Part III will discuss solutions to these issues. Solutions will include the application of the Administrative Procedure Act and the use of the Partnerships UK and BC as models for an ideal agency. Part IV will also discuss the feasibility of these solutions and hurdles to implementation.

## II. ISSUES IN APA IMPLEMENTATION

### A. *Deputization*

The first issue in APA implementation over DHS private-public partnerships is “deputization.” Deputies and deputized agents are non-governmental actors that “exerci[se] some sovereign assistance, authority, or discretion far beyond what private individuals and organizations ordinarily are

---

resources.pdf.

<sup>39</sup> PARTNERSHIPS UK, <http://www.partnershipsuk.org.uk> (last visited Apr. 7, 2013); *see also* PARTNERSHIPS BC, <http://www.partnershipsbc.ca/index.php> (last visited Apr. 7, 2013).

<sup>40</sup> *Oversight and Insight: Legislative Review of Agencies and Lessons from the States*, 121 HARV. L. REV. 613, 614-15 (2007).

permitted or expected to do.”<sup>41</sup> Deputized agents have permeated the U.S. government—“today, seemingly no transaction, whether social, political, or economic, is comfortably beyond eye or earshot of the newly deputized national security apparatchiks.”<sup>42</sup> These deputies range from the average citizen looking out for suspicious activity on his or her daily commute<sup>43</sup>, to companies turning over their consumers’ data and records to the federal government.<sup>44</sup> These arrangements are, in effect, PPPs as they leverage private and public resources together in the pursuit of the common goal of security. Deputized agents also appear in PPPs as agents who are deputized by the government to operate and accomplish the mission that the PPPs were set up for.

Activities of deputized agents range from turning over “reams of information,”<sup>45</sup> to the use of employees to “detect and report suspicious activities on the ground.”<sup>46</sup> Since the September 11th terrorist attacks, even private citizens have become deputized agents as law enforcement, security, and intelligence agencies have called upon them to prevent future harm.<sup>47</sup>

There are numerous advantages to the use of deputies. The first advantage is that they are “force multipliers” in the efforts of homeland security.<sup>48</sup> The use of private actors allows homeland security agencies to have more eyes and ears on the ground, and thus gather more information than they normally could. Furthermore, they are advantageous and cost effective because average citizens tend to be more observant of their surroundings.<sup>49</sup> Programs that utilize deputized agents include the late Highway Watch initiative, which enlisted the use of truck drivers as a set of eyes on inter- and intrastate roads<sup>50</sup>, to look for suspicious activities and crimes, such as terrorism, on national roadways.

Using normal citizens as deputized agents applies to PPPs because many

---

<sup>41</sup> Michaels, *supra* note 27 at 1442.

<sup>42</sup> *Id.* at 1435.

<sup>43</sup> U.S. DEP’T OF HOMELAND SECURITY: IF YOU SEE SOMETHING, SAY SOMETHING PUBLIC AWARENESS CAMPAIGN (last visited June 25, 2013), <http://www.dhs.gov/if-you-see-something-say-something-campaign>.

<sup>44</sup> Glenn Greenwald and Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, THE GUARDIAN, June 6, 2013, <http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data>.

<sup>45</sup> Michaels, *supra* note 27 at 1435.

<sup>46</sup> *Id.* at 1436.

<sup>47</sup> *Id.* at 1435.

<sup>48</sup> *Id.* at 1438.

<sup>49</sup> *Id.*

<sup>50</sup> *Highway Watch Going Out of Business*, TRUCKERTO TRUCKER.COM (Apr. 7, 2013, 3:37 PM), <http://www.truckertotrucker.com/trucker/1/2008/05/Highway-Watch-Going-Out-of-Business.cfm>.

of these partnerships are based on information-sharing arrangements between governments and private entities. The more casual access to private citizens, their property, and their information that comes from deputized agents can hugely benefit PPPs.<sup>51</sup> One such use of deputized citizenry in PPPs includes the famed “If You See Something, Say Something” campaign<sup>52</sup>, which asks private citizens to report information of any suspicious activity to local law enforcement agencies.<sup>53</sup> Other programs enlist the use of private police and security services as a form of PPP. These programs are actually so prevalent that the number of private security officers outnumbers the amount of public police officers in the United States by a ratio three to one.<sup>54</sup>

Additionally, on a national level, DHS works with private companies, like the NASDAQ, to address cyber threats that may be harmful to these actors—this work includes the reciprocal sharing of threats that private actors discover.<sup>55</sup> Therefore, there is a great deal of private and protected information being spread to government actors in the pursuit of homeland security. This shared information may ultimately be for the benefit of private citizens in that it keeps them safe, however, there are still major privacy concerns over this shared information based on the lack of regulation over how this information is collected and then shared.<sup>56</sup>

An example of a more direct form of deputization that threatens the privacy of private individuals is the National Security Agency’s PRISM program<sup>57</sup>, which is a prominent PPP for homeland security that has recently received national media attention. This program collects data from electronic communication companies like Facebook and Google, as well as national cell phone providers for the purpose of national security and protection of U.S.

---

<sup>51</sup> Paul Rosenzweig, *Public-Private Partnerships for Cybersecurity Information Sharing*, LAWFARE, (Sept. 2, 2012, 3:27 PM), <http://www.lawfareblog.com/2012/09/public-private-partnerships-for-cybersecurity-information-sharing/>.

<sup>52</sup> *The Department of Homeland Security at 10 Years: A Progress Report on Management: Hearing on the Challenges that Confront the Department, the Department’s Success in Implementing the Recommendations of the Government Accountability Office’s Biennial High Risk Series Update Before S. Comm. on Homeland Security and Governmental Affairs*, 112th Cong. (2013) (statement of Jane Holl Lute, Deputy Sec. of Dep’t of Homeland Security), available at <http://www.dhs.gov/news/2013/03/21/written-testimony-dhs-deputy-secretary-jane-holl-lute-senate-committee-homeland>.

<sup>53</sup> *Id.*

<sup>54</sup> Kai Jaeger and Edward P. Stringham, *Private Policing Options for the Poor*, NATIONAL CENTER FOR POLICY ANALYSIS (Dec. 15, 2011), <http://www.ncpa.org/pub/ba763>.

<sup>55</sup> Lute, *supra* note 52.

<sup>56</sup> *Id.*

<sup>57</sup> Greenwald, *supra* note 44.

citizens.<sup>58</sup>

This program can be considered a PPP because it is used for the shared interest in the pursuit of not only national, but also cyber security. The program blurs the constitutional protections of internet users because, through a private partner (Google, etc.), it allows the U.S. government access to private data regarding internet users, like search histories and online conversations without warrants and without permission from the user. This program exemplifies the fears that exist surrounding PPPs and the use of deputized agents when the U.S. government uses a private partner to circumvent various protections that surround citizens' privacy. In other words, it is not unlike a police officer having a civilian go into a private home of another in order to take papers that belong to another private citizen.

PRISM highlights not only the potential problems with PPPs, but also showcases the difficulties with the use of deputized agents. The problem is that these deputized actors enter legal spaces and gaps that are not normally assessable to conventional government officials and agents.<sup>59</sup> This includes private spaces or homes that are protected by the Fourth Amendment of the U.S. Constitution,<sup>60</sup> a challenge to which is illustrated by *United States v. Katz*,<sup>61</sup> and other cases.

On the other hand, these deputized actors also have access to powers that normally are not granted to ordinary citizens, such as the power to report on their fellow citizens with similar creditability as that of a law enforcement officer.<sup>62</sup> In other words, private citizens assume the creditability in investigating and reporting incidents that would normally be bestowed upon law enforcement officers. This is a problem because it spreads the powers of law enforcement to a body of persons that lacks the legal authority—let alone the proper training or management—to implement DHS programs in a constitutionally acceptable manner.

Finally, there are spaces and situations in between private and public realms that also pose legal questions. These questions include the following: who has a duty to report suspicious conduct; who is allowed to report misconduct; and, when is a person considered a government actor. All of these ambiguities place the deputies in a state of “limbo.”<sup>63</sup> These actors are found in “empowering, frustrating, and dangerous” states, “sometimes all at

---

<sup>58</sup> *Id.*

<sup>59</sup> Michaels, *supra* note 27 at 1437-39.

<sup>60</sup> U.S. CONST. amend. IV, § 1.

<sup>61</sup> *United States v. Katz*, 389 U.S. 347 (1967) (holding that the Fourth Amendment protects persons and not places from unreasonable intrusion).

<sup>62</sup> Michaels, *supra* note 27 at 1452-53.

<sup>63</sup> *Id.* at 1453.



once.”<sup>64</sup> In other words, many of these deputies do not know if they are government agents or not, let alone if there are regulated mechanisms to address abuses that they may carry out.<sup>65</sup> The deputized actors who participate in PPPs need better governance to prevent constitutional,<sup>66</sup> and other abuses.<sup>67</sup>

### B. *Excessive Congressional Oversight*

The Homeland Security Act of 2002 (“HSA”) provides that the U.S. House of Representatives and Senate have legislative oversight over the Department of Homeland Security.<sup>68</sup> While the oversight it is constitutionally mandated and necessary to maintain checks and balances over DHS<sup>69</sup>, the problem is that the oversight has become too burdensome.<sup>70</sup>

Specifically, the U.S. House of Representatives and Senate have 108 different committees and subcommittees that have some oversight role over the Department of Homeland Security.<sup>71</sup> These committees range from the relevant House Homeland Security Committee to the less obviously relevant Select Committee on Aging.<sup>72</sup> In one year, some 3,900 briefings were brought to Congress, wherein it asked DHS to testify before various committees 285 times.<sup>73</sup> These oversight measures are estimated to have cost DHS thousands of man-hours, not to mentioned “tens of millions of dollars.”<sup>74</sup> Although this oversight is necessary for such a large and expansive department like DHS, and is constitutionally mandated, the current system is excessive.<sup>75</sup>

According to Paul Schneider, the former Deputy Secretary of Homeland Security, within his first ten months on the job at DHS he was called to testify on Capitol Hill nine times.<sup>76</sup> Schneider explains that he spent many hours

---

<sup>64</sup> *Id.*

<sup>65</sup> *Id.*

<sup>66</sup> *Id.*

<sup>67</sup> *Id.*

<sup>68</sup> Homeland Security Act of 2002, P.L. 107-296, 107th Cong. (2002).

<sup>69</sup> U.S. CONST. amend. I, § 8.

<sup>70</sup> Carafano, *supra* note 25.

<sup>71</sup> *Id.*

<sup>72</sup> Koempel, *supra* note 34.

<sup>73</sup> National Security Preparedness Group, *supra* note 24.

<sup>74</sup> Jessica Zuckerman, *Politics Over Security: Homeland Security Congressional Oversight In Dire Need of Reform*, THE HERITAGE FOUNDATION (Sept. 10, 2012), [http://www.heritage.org/research/reports/2012/09/homeland-security-congressional-oversight-in-dire-need-of-reform#\\_edn3](http://www.heritage.org/research/reports/2012/09/homeland-security-congressional-oversight-in-dire-need-of-reform#_edn3).

<sup>75</sup> U.S. DEP’T OF HOMELAND SECURITY, ORGANIZATION CHART (last visited Mar. 5, 2013), <http://www.dhs.gov/xlibrary/assets/dhs-orgchart.pdf>.

<sup>76</sup> Katherine McIntire Peters, *Congressional Oversight in Homeland Security*, THE GOVERNMENT EXECUTIVE (July 30, 2008), <http://www.govexec.com/federal->

preparing for these hearings, and then was unable to spend time working on actual homeland security issues.<sup>77</sup> Further, because of the diversity of oversight committees, many of these hearings and testimonies can be extremely redundant and thus waste even more time.<sup>78</sup> According to one news report, DHS spent 66 work years responding to questions from Congress in 2009 alone.<sup>79</sup> Additionally, that same year DHS "answered 11,680 letters, gave 2,058 briefings and gave 2,058 briefings and sent 232 witnesses to 166 hearings."<sup>80</sup> This all cost American taxpayers some \$10 million in one year.<sup>81</sup>

This issue is so serious that, in September 2007, Homeland Security Secretary Chertoff wrote a letter to then-Ranking Member of the House Homeland Security Committee.<sup>82</sup> This letter detailed "literally thousands of congressional requests – from many different committees and subcommittees for hearings, briefings, reports and other information – [that] consume a very significant amount of DHS senior leadership time, which must be balanced with meeting operational mission demands."<sup>83</sup>

In comparison, a 2004 whitepaper jointly authored by the Center for Strategic and International Studies and Business Executives for National Security showed that the Department of Defense, a significantly larger executive department than the Department of Homeland Security, reports to only 36 congressional committees or subcommittees, versus the 108 that manage the Department of Homeland Security.<sup>84</sup>

Homeland security is being muddled by this redundant accountability.<sup>85</sup> The multitude of congressional committees also preserves the fragmentation that the Department of Homeland Security was supposed to dissolve when the 22 agencies were brought together under the Homeland Security Act of 2002

---

news/2008/07/congressional-oversight-of-homeland-security-comes-under-fire-again/27357/.

<sup>77</sup> National Security Preparedness Group, *supra* note 24.

<sup>78</sup> *Id.*

<sup>79</sup> *Homeland Security Department Overwhelmed by Congressional Oversight*, FOX NEWS, May 17, 2011, <http://www.foxnews.com/politics/2011/05/17/homeland-security-department-overwhelmed-congressional-oversight/>.

<sup>80</sup> *Id.*

<sup>81</sup> *Id.*

<sup>82</sup> National Security Preparedness Group, *supra* note 24.

<sup>83</sup> *Id.*

<sup>84</sup> A Whitepaper of the CSIS-BENS Task Force on Congressional Oversight of the Dep't of Homeland Security [hereinafter CSIS-BENS Whitepaper], *Untangling the Web: Congressional Oversight and the Department of Homeland Security*, CENTER FOR STRATEGIC AND INT'L STUDIES (Dec. 10, 2004), available at [http://csis.org/files/media/csis/events/041210\\_dhs\\_tf\\_whitepaper.pdf](http://csis.org/files/media/csis/events/041210_dhs_tf_whitepaper.pdf).

<sup>85</sup> National Public Radio Staff [hereinafter NPR Staff], *Who Does Not Oversee Homeland Security?*, NAT'L PUB. RADIO, Jul. 10, 2010, <http://www.npr.org/templates/story/story.php?storyId=128642876>.

("HSA").<sup>86</sup> In other words, the multitudes of committees are counterintuitive to the purpose of the HSA.<sup>87</sup> This is because the HSA was drafted for the purpose of centralization, whereas the myriad of congressional committees is counterintuitive to this very idea.

There are many reasons for these legislative impediments, ranging from the fact that members of Congress like having the credentials of sitting on a Homeland Security Committee, to inter-committee "turf wars."<sup>88</sup> The problem is so severe that former Chairman of the Senate Homeland Security and Government Affairs Committee, Joe Lieberman, believed that reform could not come from the legislative branch because of how the Department of Homeland Security was formed.<sup>89</sup> DHS was not built from the ground up; rather it was built out of existing organs and offices.<sup>90</sup> These preexisting agencies and offices already had congressional committees overseeing them.<sup>91</sup> When DHS was created by merging preexisting agencies, members of Congress were hesitant to give up their powerful committee assignments.<sup>92</sup> Because Congress is hesitant to acquiesce its power over those agencies, a solution to the problem of over-governance of the DHS must come from the executive branch.<sup>93</sup>

### C. Management and Accountability

Another major issue facing the future of private-public sector partnerships in homeland security relates to the command and control mechanisms for PPPs that will allow them to be properly managed and held accountable.<sup>94</sup> There seems to be a dichotomy between the governance style as it moves away from a "paramilitary-style, top-down structure,"<sup>95</sup> to network

---

<sup>86</sup> The Department of Homeland Security was formed by Homeland Security Act of 2002 in response to the September 11, 2001 attacks. From its inception it was designated as an executive department designated to prevent, minimize, and handle manmade and natural disasters. The 2002 legislation also brought 22 different agencies under the same department from a variety of several executive departments. See U.S. DEP'T OF HOMELAND SECURITY, *Creation of the Department of Homeland Security*, available at <http://www.dhs.gov/creation-department-homeland-security>.

<sup>87</sup> *Id.*

<sup>88</sup> NPR Staff, *supra* note 85.

<sup>89</sup> *Id.*

<sup>90</sup> U.S. DEP'T OF HOMELAND SECURITY, *supra* note 86.

<sup>91</sup> NPR Staff, *supra* note 85.

<sup>92</sup> *Id.*

<sup>93</sup> *Id.*

<sup>94</sup> Nathan E. Busch and Austen D. Givens, *Public-Private Partnerships in Homeland Security: Opportunities and Challenges*, 8 HOMELAND SECURITY AFFAIRS 10 (2012).

<sup>95</sup> *Id.*

governance.<sup>96</sup>

"Network governance" is the management of agencies and programs in a "flatter," less hierarchical form, which rejects the notion of one organ, person, or group having power over another.<sup>97</sup> Everyone is an equal player in network governance.<sup>98</sup> At the same time, as identified by Senator Joseph Lieberman, there needs to be someone in charge when dealing with both private and public actors.<sup>99</sup> Some authorities and policy makers advocate for the federal government to always be the ultimate authority in homeland security partnerships and contracting.<sup>100</sup> There seems to be an ongoing debate between legislators, government managers, and the private sector with no clear direction.<sup>101</sup> Hence, a major component to the private-public overlay is control.<sup>102</sup>

The final issue deals with accountability,<sup>103</sup> specifically who is reporting to whom, and who is able to testify on behalf of a specific PPP to Congress. Currently, these partnerships (especially in DHS) are scattered and governed by assorted councils, offices, and agencies.<sup>104</sup> The current structure makes this not just an issue of decentralized management, but also accountability that must be remedied.

### III. SOLUTIONS

#### A. Overview

A solution to these problems is centralization. DHS should have a single agency that implements, manages, and creates rules for all PPPs within the department. Developing such an umbrella organization promises to be a challenge in this particular case because there are both private and public stakeholders who desire an equal place at the governing table. One way to ensure the equality of both the public and private stakeholders is to use a

---

<sup>96</sup> *Id.*

<sup>97</sup> THE PROGRAM ON NETWORKED GOVERNANCE,  
<http://www.hks.harvard.edu/netgov/html/index.htm> (last visited Apr. 7, 2013).

<sup>98</sup> *Id.*

<sup>99</sup> Gregg Carlstorm, *DHS budget Begins 'Turnaround' Away From Contracting*, FEDERAL TIMES (Feb. 24, 2010, 1:33 PM),  
<http://www.federaltimes.com/article/20100224/CONGRESS03/2240304/1055/AGENCY>.

<sup>100</sup> *Id.*

<sup>101</sup> Stephen Losey, *TSA Halts Expansion of Privatized Airport Screening*, FEDERAL TIMES (Jan. 31, 2011, 6:00 PM),  
<http://www.federaltimes.com/article/20110131/DEPARTMENTS03/101310303/1050/PERSONNEL04>; see also Busch, *supra* note 94.

<sup>102</sup> Busch, *supra* note 94.

<sup>103</sup> *Id.*

<sup>104</sup> U.S. DEP'T OF HOMELAND SECURITY, DEPARTMENT-WIDE RESOURCES, *supra* note 38.

governance model similar to that of the late Partnerships UK and Partnerships BC, in the United Kingdom and British Columbia, Canada, respectively. Under these models, these agencies are set up to govern and oversee all PPPs in their specific area of governance.<sup>105</sup> In the words of the Partnerships BC website, it carries out the “planning, delivery and oversight of . . . projects.”<sup>106</sup> It goes on to state that Partnerships BC uses relationships with both private and public partners in order to complete its mission.<sup>107</sup> This model includes an executive board<sup>108</sup>, which has members from the relevant government body.<sup>109</sup> Additionally, there would be an advisory council that ensures that issues are discussed by the executive board.<sup>110</sup> In other words, the advisory council makes sure the office keeps to its mission.<sup>111</sup> Finally, like a private sector actor, the office issues annual reports and has corporate responsibility policies.<sup>112</sup>

This system is admirable and provides a great template for PPP governance in DHS. However, like all solutions, this one is not perfect. There are a number of issues that arise with the implementation of such a system, although there are ways to mitigate those problems.

A proposed framework would be as follows for the new umbrella agency. First, like Partnerships UK, it would have two boards of oversight: one advisory, and one of directors.<sup>113</sup> Both boards would include public and private sector representatives as members, to ensure that all stakeholders have input. Additionally, this board of directors would have oversight over a management team, which would consist of professional government bureaucrats. They would then report to and the CEO would be accountable to Congress, as well as the board of directors. Thus, DHS would adopt the accountability structure, at least partially, from Partnerships BC.<sup>114</sup> Finally, in light of the need for a unified liaison in times of emergency, the CEO will function as unified decision-maker just like any director or chief administrator in the federal government.<sup>115</sup>

These boards, as illuminated in the charters of Partnerships UK and

---

<sup>105</sup> PARTNERSHIPS BC, <http://www.partnershipsbcc.ca/index.php> (last visited Apr. 7, 2013).

<sup>106</sup> *Id.*

<sup>107</sup> *Id.*

<sup>108</sup> In the case of an American model, the government body would be the Department of Homeland Security.

<sup>109</sup> PARTNERSHIPS UK, GOVERNANCE AND BOARD, <http://www.partnershipsuk.org.uk/Governance-and-Board.aspx> (last visited Apr. 7, 2013).

<sup>110</sup> *Id.*

<sup>111</sup> *Id.*

<sup>112</sup> *Id.*

<sup>113</sup> *Id.*

<sup>114</sup> PARTNERSHIPS BC, *supra* note 105.

<sup>115</sup> 42 U.S.C.A. § 1983 (1996).

Partnerships BC, should be kept, but with minor changes. One is to incorporate private partners on to the advisory board, ensuring that they have an equal stake at the table. Second, the board should have a chairperson that is appointed by the executive branch, much like any other administrator in the federal government, with the conventional congressional confirmation process. Another solution would be in the creation of a chief executive officer ("CEO"), not unlike that in Partnerships BC.<sup>116</sup> This position could be created under the appointment power of the U.S. Constitution.<sup>117</sup> Another choice could be to adopt the entire Partnerships BC model where there is a board of directors and a management team.<sup>118</sup> This allows the additional oversight based on criteria drafted by the board and the CEO, wherein CEO performance is evaluated.<sup>119</sup>

This note proposes that the Partnerships BC model should be adopted with both a CEO and board chair. This model will allow a point of contact that Congress can address in hearings, or any other oversight mechanism. The CEO is also crucial in creating a point person within DHS with absolute authority in times of emergency or crisis, a situation that is particularly important in a department like DHS that deals with some of the U.S.'s most serious emergencies.

This more centralized management of PPPs should be governed like any other agency under the APA.<sup>120</sup> This means that for purposes of oversight, Congress would call the head of each of these partnerships rather than Secretary of Homeland Security's office or the Secretary herself to testify.<sup>121</sup> The act of this transfer of power has a dual advantage. The first advantage is that it will create more central oversight of private-public partnerships by Congress, thus eliminating redundancy in congressional hearings, meetings, and testimony that waste resources.<sup>122</sup> The second advantage is that it creates a more centralized system to manage the PPPs themselves. Finally, this agency will be able to make rules like any other agency as provided under the APA. These rules will be passed in order to govern all the partnerships, specifically to allow proper planning, management, and operations of the PPPs.

---

<sup>116</sup> PARTNERSHIPS BC, MANAGEMENT TEAM, <http://www.partnershipsbcc.ca/files-4/management-team.php> (last visited Apr. 7, 2013).

<sup>117</sup> U.S. CONST. art. 2, § 2.

<sup>118</sup> PARTNERSHIPS BC, *supra* note 105.

<sup>119</sup> *Id.*

<sup>120</sup> Administrative Procedure Act (APA), 5 U.S.C. § 500 (1946).

<sup>121</sup> Administrative Procedure Act (APA), 5 U.S.C. § 552b (1946).

<sup>122</sup> CSIS-BENS Whitepaper, *supra* note 84.

### B. *Deputization*

There needs to be some sort of accountability that governs deputies, and holds them accountable when problems arise, whether through abuse of constitutional rights or by corruption. To continue implementing deputized citizens under DHS, a program must be created in order to protect U.S. citizens from the potential abuses of these private, but deputized, actors. These abuses could include illicit entry into private homes,<sup>123</sup> or collection of personal communication through national telecommunication companies.<sup>124</sup>

Currently, this problem has been addressed in limited ways, such as in Executive Order 13636: Improving Critical Infrastructure Cybersecurity.<sup>125</sup> In this executive order, the executive branch acknowledged that the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security should advise the Secretary of the Department of Homeland Security about possible issues with deputization, such as violations of civil liberties and unauthorized access to private realms.<sup>126</sup> Finally, even though the entire Department of Homeland Security has a Privacy Office, which is “responsible for evaluating Department programs, systems, and initiatives for potential privacy impacts, and providing mitigation strategies to reduce the privacy impact,”<sup>127</sup> there needs to be even more oversight specifically detailed to PPPs.

There are many internal controls, but not many specific avenues for a private citizen, actor, or organization to traverse.<sup>128</sup> There is also the issue of private actors, like a cable repairman who relays constitutionally protected information to government agents. Does the private party file a suit as outlined in 42 U.S.C. § 1983?<sup>129</sup> This statute states that a person whose constitutional rights are infringed upon by an actor under the color of law is entitled to seek injunctive relief those rights infringements.<sup>130</sup> The U.S. Supreme Court has ruled in some of these cases using 42 U.S.C. § 1983 as its basis, including *Barton Protective Services, Inc. v. Faber*.<sup>131</sup> In this case, mall

---

<sup>123</sup> Michaels, *supra* note 27 at 1444.

<sup>124</sup> Greenwald, *supra* note 44.

<sup>125</sup> Exec. Order No. 13636, 78 Fed. Reg. 33 (Feb. 19, 2013), *available at* <http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf>.

<sup>126</sup> *Id.*

<sup>127</sup> U.S. DEP’T OF HOMELAND SECURITY, ABOUT THE PRIVACY OFFICE, <http://www.dhs.gov/about-privacy-office> (last visited Apr. 7, 2013).

<sup>128</sup> U.S. DEP’T OF HOMELAND SECURITY, DHS PRIVACY OFFICE GUIDE TO IMPLEMENTING PRIVACY, <http://www.dhs.gov/sites/default/files/publications/privacy/Reports/dhsprivacyoffice-guidetoimplementingprivacy.pdf> (last visited Apr. 8, 2013).

<sup>129</sup> 42 U.S.C.A. § 1983 (1996).

<sup>130</sup> *Id.*

<sup>131</sup> *Barton Protective Servs., Inc. v. Faber*, 745 So. 2d 968, 970 (Fla. Dist. Ct. App. 1999).

patrons sued Barton Protective Services, Inc. and police officers for malicious prosecution, false arrest, and violations of § 1983.<sup>132</sup> The patrons were successful in the suit on the ground that the private security forces were acting as deputized state actors, hence they were liable under state action theory.<sup>133</sup> This analysis was clear for those who are obviously acting as state actors, such as mall security officers<sup>134</sup>, but what about the above-mentioned cable repairman? Does a private citizen file a § 1983 suit against the cable repairman for reporting suspicious activity in their private home, against the cable company for sending this information to law enforcement authorities, or the law enforcement agency itself?

This is where administrative law can be usefully applied to private-partnerships and their agents. In constitutional law, there is a mechanism called state action. State action is the principle by which anything done by a government that is an intrusion on a person's civil rights by a government agent or private actor under government orders, the intrusion must come from a governmental action.<sup>135</sup> This government action can be anything from a restrictive covenant to prevent certain behaviors, to judicial action to enforce constitutional protections.<sup>136</sup> These constitutional protections include the protection from warrantless search and seizure<sup>137</sup> and due process of law.<sup>138</sup>

This concept can be applied to deputies within private-public sector partnerships.<sup>139</sup> The government can use these deputies as "private proxies,"<sup>140</sup> who carry out government actions to expand the coverage and scope of counterterrorism activities.<sup>141</sup> The problem therein, though, is that these proxies can obtain information and enter spaces that normal government actors cannot.

In order to fill this gap in oversight and judicial "reining-in" of deputized actors, there needs to be a clearer definition of who is a government actor and when they are and are not functioning as a government actor. The best solution is to adopt the wiretap court model created under the Foreign Intelligence Surveillance Act of 1978 ("FSIA").<sup>142</sup> This 1978 legislation called for the use of a panel of three judges, which are appointed by the U.S. Supreme

---

<sup>132</sup> *Id.*

<sup>133</sup> *Id.*

<sup>134</sup> *Id.*

<sup>135</sup> Bryan A. Garner, BLACK'S LAW DICTIONARY 1538 (perm. ed. 2009).

<sup>136</sup> *Id.*

<sup>137</sup> U.S. CONST. amend. IV.

<sup>138</sup> U.S. CONST. amend. V; U.S. CONST. amend. XIV.

<sup>139</sup> Michaels, *supra* note 27 at 1461.

<sup>140</sup> *Id.* at 1463-64.

<sup>141</sup> *Id.*

<sup>142</sup> 50 U.S.C.A. §§ 1803-1805.



Court.<sup>143</sup> The purpose of this court is to deny or affirm applications for wiretaps.<sup>144</sup>

A similar court should be set up for the purposes of information exchanges between private and public partners within homeland security situations. This court should always meet when private information will be exchanged with public entities. The court should also rule if private actors are considered government agents. If the court confirms that a private actor is in fact a government agent, then such an agent should be subject to all the accountability statutes and rules concerning government agents including § 1983 claims. Though this may be a cumbersome undertaking, it is a necessary step in protecting the civil liberties and rights of U.S. citizens.<sup>145</sup>

### C. *Excessive Congressional Oversight*

Current solutions that are being proposed to solve congressional oversight issues come from a variety of sources. One proposal is to streamline the myriad committees to a few, more specific, committees<sup>146</sup>, or one larger committee.<sup>147</sup> Other proposals include making a joint committee, that is one with members from both the Senate and House of Representatives, who represent all of the committees that have authorization powers over the Department of Homeland Security.<sup>148</sup> The problem with these solutions is that they are creations and developments of the legislative branch. As detailed above, legislative programs are not easy to implement for a variety of reasons<sup>149</sup>, which include, *inter alia*, congressional turf wars and the desire of members of Congress to hold on to their powerful committee seats. These impediments make legislative solutions less likely to succeed.

An alternative to legislative branch-based solutions, which could cut down on this congressional gridlock and excessive oversight, is the application of the Administrative Procedure Act (“APA”). Specific legislation would allow the creation of a stand-alone agency for PPPs to report to. This means that Congress would only have a single agency to oversee in the form of the oversight agency, instead of vastly complex agency it currently deals with. Numerous councils, panels, and committees that currently govern PPPs in the Department of Homeland Security would also be eliminated.<sup>150</sup> By creating an

---

<sup>143</sup> 50 U.S.C.A. § 1803.

<sup>144</sup> *Id.*

<sup>145</sup> *Id.*

<sup>146</sup> Carafano, *supra* note 25.

<sup>147</sup> CSIS-BENS Whitepaper, *supra* note 84.

<sup>148</sup> Carafano, *supra* note 25.

<sup>149</sup> *Id.*

<sup>150</sup> U.S. DEP’T OF HOMELAND SECURITY, NATIONAL INFRASTRUCTURE PROTECTION PLAN: PARTNERING TO

independent agency, a focal point for congressional accountability and related activities (such as official testimonies and hearings) would be created. Instead of multiple officers being hailed to Capitol Hill and constantly having to compile reports, there would only be one set of officers and one set of staff reporting to Congress. The reasoning for this is that currently PPPs are being governed by a multitude of agencies, councils, and offices. Creating one centralized source of PPPs within DHS has several advantages. First, by placing PPPs under one agency, it takes power away from these vast agencies, councils, and offices. This means that when these oversight bodies are dissolved it will eliminate the multiple congressional oversight committees that currently have jurisdiction. Additionally, placing one organization in charge of PPPs will allow for proper expansion of the use of PPPs, and also proper regulatory oversight of these PPPs.<sup>151</sup>

This more centralized management of these partnerships should be governed like any other agency under the APA.<sup>152</sup> This means that Congress, for purposes of oversight, would call the head of each of these partnerships rather than the Secretary of Homeland Security's office, or the Secretary herself, to testify.<sup>153</sup> The act of this transfer of power has a dual advantage. The first advantage is that it will create more centralized oversight of private-public partnerships by Congress, thus eliminating redundancy in congressional hearings, meetings, and testimony, which wastes so many resources of time, personnel, and money.<sup>154</sup> The second advantage is that the transfer of power creates a more centralized system to manage the private-public sector partnerships themselves. Finally, this agency will be able to make rules like any other agency as provided under the APA.

#### D. *Management and Accountability Problems*

Not only does implementing the APA solve issues with congressional oversight, but it also rectifies management and accountability problems. By centralizing the governance of PPPs, management and accountability would be streamlined and centralized in order to implement DHS's goals.<sup>155</sup>

There are several facets of standardizing the use of PPPs.<sup>156</sup> The first is to

---

ENHANCE PROTECTION AND RESILIENCY, 2009, *available at* [http://www.dhs.gov/xlibrary/assets/NIPP\\_Plan.pdf](http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf).

<sup>151</sup> Gaffey, *supra* note 37.

<sup>152</sup> Administrative Procedure Act (APA), 5 U.S.C. § 500 (1946).

<sup>153</sup> Administrative Procedure Act (APA), 5 U.S.C. § 552b (1946).

<sup>154</sup> NPR Staff, *supra* note 85.

<sup>155</sup> Gaffey, *supra* note 37.

<sup>156</sup> *Id.*

promote the use and expansion of PPPs.<sup>157</sup> Promotion includes the education of the public, public actors, and private actors.<sup>158</sup> By allowing all players to know the benefits of using PPPs, their use will be expanded. Education will also allow partnerships to have a better understanding of the whole partnership and not just their own interests. This will allow better cooperation and participation on behalf of all parties.

Also, the specific umbrella agency should be tasked with creating rules for governance and oversight of these partnerships.<sup>159</sup> This means that this agency should function like any other government office or organ when it is empowered by the APA. In other words, this umbrella agency should be able to make rules that carry the force of law.<sup>160</sup> Also, this agency should be able to hold administrative hearings to address claims and disputes that arise from its conduct.<sup>161</sup> Finally, as David W. Gaffey points out, this office should have oversight over all of partnerships including “accounting, auditing, legal, and contract management oversight.”<sup>162</sup> By adopting these principles, this umbrella agency will be able to govern private-public sector partnerships through their entire life span<sup>163</sup>, including any challenges that the ever-changing nature of homeland security will create for it.<sup>164</sup>

This umbrella agency should be implemented through specific statutes made by Congress<sup>165</sup>, not through agency made rules (from the Department of Homeland Security). It should be chartered, authorized, and empowered by the legislative branch even though it will operate under the auspices of DHS. It will therefore have legislative and executive recognition and control like any other constructed agency under the executive branch as empowered by the Constitution.<sup>166</sup> Therefore on paper this agency will look, act, function, and be overseen like the Federal Aviation Administration or any other executive agency.<sup>167</sup> By adopting this model, the new umbrella agency will be afforded

---

<sup>157</sup> *Id.*

<sup>158</sup> *Id.*

<sup>159</sup> *Id.*

<sup>160</sup> 5 U.S.C. 553 (1947).

<sup>161</sup> 5 U.S.C. 556 (1947).

<sup>162</sup> Gaffey, *supra* note 37.

<sup>163</sup> *Id.*

<sup>164</sup> U.S. DEP'T OF HOMELAND SECURITY, QUADRENNIAL HOMELAND SECURITY REVIEW REPORT, Feb. 2010, available at

[http://www.dhs.gov/xlibrary/assets/qhsr\\_report.pdf](http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf).

<sup>165</sup> Alfred C. Aman Jr., *Privatization and the Democracy Problem in Globalization: Making Markets More Accountable Through Administrative Law*, 28 FORDHAM URB. L.J. 1477, 1501 (2001).

<sup>166</sup> U.S. CONST. art. 1, § 8.

<sup>167</sup> FED. AVIATION ADMIN., A BRIEF HISTORY OF THE FAA,

greater legitimacy, less fragmentation, and one centralized authority, which Congress, the executive branch, and other regulatory bodies can oversee.<sup>168</sup>

#### IV. BENEFITS OF APA IMPLEMENTATION

This plan for a centralized agency to manage all PPPs will solve the current issues in DHS. This is because it is a reform project that is not without precedent. The late Partnerships UK and Partnerships BC serve as precedents to this type of overhaul. Additionally, this is not a wholly new concept to the U.S. government, or even to DHS. Currently, DHS has initiatives that do similar, if not identical tasks. Initiatives like the "SECURE" (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program and its "sister project" called "FutureTECH,"<sup>169</sup> streamline DHS's ability to acquire products, and implement policies and procedures from the private sector for its own uses.<sup>170</sup>

Although acquisition is not the same as a partnership for the purposes of this note, the concept of the interaction of federal and private actors is similar. On the other hand, some programs, like National Protection and Programs Directorate, Office of Infrastructure Protection, are not as scattered.<sup>171</sup> The National Protection and Programs Directorate, Office of Infrastructure Protection, is much more regulated, uniform in control mechanisms, and includes proper oversight mechanisms from the both the private and public sides.<sup>172</sup> The problem here, however, is that this program only covers a small percentage of the total PPPs under the auspices of homeland security.

Because there are vast numbers of agencies throughout the federal government that use the APA to draft, vet, and implement rules governing initiatives and that carry the force of law, the APA will prove effective in this vein. Therefore applying this ubiquitously used statute to DHS should pose less of a problem than creating an untried and untested means of solving this issue.

---

[http://www.faa.gov/about/history/brief\\_history/](http://www.faa.gov/about/history/brief_history/) (last visited Apr. 7, 2013).

<sup>168</sup> Aman, *supra* note 165.

<sup>169</sup> U.S. DEP'T. OF HOMELAND SECURITY, SYSTEM EFFICACY THROUGH COMMERCIALIZATION, UTILIZATION, RELEVANCE AND EVALUATION (SECURE), <http://www.dhs.gov/secure-system-efficacy-through-commercialization-utilization-relevance-and-evaluation-program> (last visited Mar. 5, 2013).

<sup>170</sup> Thomas A. Cellucci, *System Efficacy through Commercialization, Utilization, Relevance and Evaluation (SECURE) Program: Concept of Operation*, U.S. DEP'T. OF HOMELAND SECURITY, *available at*

[http://www.dhs.gov/xlibrary/assets/secure\\_program\\_overview\\_and\\_concept\\_of\\_operations.pdf](http://www.dhs.gov/xlibrary/assets/secure_program_overview_and_concept_of_operations.pdf).

<sup>171</sup> U.S. DEP'T. OF HOMELAND SECURITY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE: OFFICE OF INFRASTRUCTURE PROTECTION STRATEGIC PLAN: 2012-2016 (Aug. 2012), *available at* <https://www.dhs.gov/sites/default/files/publications/IP%20Strategic%20Plan%20FINAL.pdf>.

<sup>172</sup> *Id.*

Finally, the federal government, including DHS, has already followed this model in a limited fashion. This precedent can be found in the post-September 11th U.S. Coast Guard's program for port security.<sup>173</sup> This program was initiated soon after September 11th when U.S. government officials realized that more than 360 ports were vulnerable to terrorist attacks.<sup>174</sup> This is tremendously important as 95% of imports come into the United States come by sea, making them a focal point of the U.S. economy.<sup>175</sup>

As a result of these vulnerabilities, Congress passed the Marine Transportation Security Act in an attempt to secure the ports.<sup>176</sup> The monumental task of passing the legislation to secure the ports was assigned to the U.S. Coast Guard.<sup>177</sup> One of the major problems that the Coast Guard wanted to avert was slowing, stalling, or even stopping international maritime commerce at ports due to too stringent security measures.<sup>178</sup> The Coast Guard feared that there would be too many agencies and offices, and that they would "gum up" trade with too many checks and investigations.<sup>179</sup> Another consideration was the because of the diversity of ports and facilities there could be ports with different policies and practices, making one uniform plan impossible.<sup>180</sup> Therefore, some other solution had to be found.

As a result, under the APA, a series of meetings were held across the country as a form of standard review-and-comment sessions, as provided for in the statute.<sup>181</sup> Both stakeholders (port operators, etc.) and officials (federal government officials) brought to the table their own priorities and standards, which had to be met.<sup>182</sup> Eventually, they came together with a definitive plan that met the needs and wants of all the parties.<sup>183</sup>

The plan used established standards of security, which were issued and enforced by the Coast Guard and the U.S. government.<sup>184</sup> Private parties (the ports) enforced those standards, while their contractors (the ports' contractors) carried out the standards that were established.<sup>185</sup> In other words, the private actors implemented plans customized by the government—

---

<sup>173</sup> DONAHUE, *supra* note 10, at 64.

<sup>174</sup> *Id.* at 64-65.

<sup>175</sup> *Id.*

<sup>176</sup> *Id.*

<sup>177</sup> *Id.*

<sup>178</sup> *Id.*

<sup>179</sup> *Id.*

<sup>180</sup> *Id.*

<sup>181</sup> *Id.*

<sup>182</sup> *Id.*

<sup>183</sup> *Id.*

<sup>184</sup> *Id.*

<sup>185</sup> *Id.*

the perfect example of a PPP.<sup>186</sup> There were some suspicions about the viability and efficacy of this plan<sup>187</sup>; however, subsequent independent studies, including those from the Government Accountability Office, have proved those suspicions to be unfounded. Those studies have shown that this PPP has been an effective means of homeland security.<sup>188</sup> Thus, this provides an example of a well-run PPP crafted using provisions of the APA.

#### V. CONCLUSION

In conclusion, by turning to the use of PPPs the U.S. government will be able to address the ever-changing nature of homeland security.<sup>189</sup> These challenges can be addressed through the use of PPPs, but in their current incarnation these partnerships are not properly governed and managed. The problems that plague the current PPP system within the DHS include deputization, excessive congressional oversight, and improper management and accountability mechanisms. All of these problems can be solved with the application of an umbrella agency that manages all the PPPs under one office within the DHS, instead of the multitude of offices that currently do. Additionally, in order to even further standardize these PPPs they should all governed under rules formed by the APA.



---

<sup>186</sup> *Id.*

<sup>187</sup> *Id.*

<sup>188</sup> *Id.*

<sup>189</sup> Carafano, *supra* note 25.

## Book Review

### **Terrorism, Ticking Time-Bombs, and Torture: A Philosophical Analysis**

By Fritz Allhoff

*Reviewed by Krysta Ku*

Professor Fritz Allhoff is more than well versed in the ethics of terrorism and torture. He has travelled to numerous universities in the United States and abroad, giving presentations on the moral status of interrogational torture. In addition, in 2009, Allhoff led a graduate seminar entitled “War, Terrorism, and Torture”; his articles on the topic, including his most recent article, “Torture Warrants, Self Defense, and Necessity,” have been published in various law and philosophy journals. Allhoff is currently an Associate Professor in the Department of Philosophy at Western Michigan University and a Senior Research Fellow at The Australian National University’s Centre for Applied Philosophy and Public Ethics. In the midst of his professional and academic pursuits and accomplishments, Allhoff successfully authored the book, *Terrorism, Ticking Time-Bombs, and Torture: A Philosophical Analysis*.

In his work, Allhoff asks the reader to answer this question honestly: “If interrogational torture is necessary for the abrogation of some terrorist threat, would that torture be justified?” He not only adeptly tackles this question, but he also provides a comprehensive framework for doing so. While this is the direct question his work deals with, Allhoff first equips the reader with a discussion on terrorism and torture before delving into the ticking time-bomb question. Although the reader may be anxious to read arguments for the necessity and justification of interrogational torture, such apprehensions are unjustified. Allhoff impeccably proves that in order for one to understand these arguments, one must understand modern terrorism, torture, and America’s connection to, and status on, both.

In effect, Allhoff’s book began with the 9/11 attacks and the Bush administration’s response to them. He delves into how the 9/11 attacks set a ripple effect into motion, including the triggering of the War on Terror, the passage of the Patriot Act, and the creation of the Department of Homeland Security. This necessary background leads to an argument, which in the current political and cultural climate is particularly intriguing: whether the Bush Administration really failed. While one ponders this question, Allhoff reminds the reader that there hasn’t been an act of terrorism on U.S. soil for over 10 years. While many works jump at the chance to criticize the Bush

Administration and its response to 9/11, Allhoff challenges the reader to take a step back and examine the response and the outcome more closely.

He states that "in some relevant sense, Bush's strategies worked." So, the real question was whether the means justified the ends. Or, in other words, were Bush's strategies necessary or justified, and was the cost to ensure our safety justified? Allhoff shows that these questions are really part of a bigger philosophical question about what we can do to protect ourselves.

Allhoff provides a utilitarian approach on contemporary torture and the ticking time-bomb theory. He explains that "lesser harms are preferable to greater harms, and in exceptional cases torture can be the lesser harm." To bolster this argument, Allhoff points out that the current torture debate is too fixated on the tortured and not enough on the people who are threatened by terrorist attacks. In contrast, he approaches the torture debate "by placing a premium on the lives of innocents—rather than the putative rights of suspected terrorists." This viewpoint on torture is significantly transformed when changing focus. Thus, even if torture has a moderate or low chance of saving a significant number of lives, in Allhoff's view this is a reasonable option we should consider.

In order to fully expand and develop his position on the torture of terrorists during interrogation, Allhoff separated his work into three parts. Part I focuses entirely on terrorism—its definition, the reasons for its evilness, and how the contemporary advent of terrorism has changed traditional norms. Part II heavily discusses torture, its definition, and reasons for why it is intrinsically wrong. In Part III, Allhoff goes beyond the philosophical discourse to discuss real world application of the ticking-time bomb theory.

Not only are his arguments based in logic, but Allhoff's work is also laid out in a coherent format, where each part of the book builds off of, and expands upon, a previous part. Professor Allhoff's book has voiced a rare and lacking view on interrogational torture in a vacuum of literature decrying its use. His book also serves a dual function of explaining his position, as well as responding to the positions on torture of other scholars. He leaves politics out of the discussion, and purely focuses on the philosophical and empirical treatments of torture and ticking-time bomb cases. Most importantly, the book is guided by the idea that innocent lives come first, not the lives of those being interrogated.

When reading this book, it is important to understand that Allhoff recognizes that torture is filled with moral harms; he has no argument in that. Allhoff adamantly defines the limits of torture. He asserts that torture is not a panacea, insofar as ticking time-bomb cases are exceptional. He clearly is not advocating widespread, institutionalized torture, nor unwarranted torture. Instead, he asserts that torture must be used when necessary or prudent. He



also points out that torture does not address causes of terrorism, but “is at best a temporary solution to a deeper problem.” Ultimately, he suspects “that torture would ever be justified only in cases reasonably close to ticking-time-bomb cases and that the torture of innocents and preventative torture are not likely to recommend themselves.”

Terrorism also poses serious moral harms—harms that we have the ability to defend against. Although torture may not be the best way of defense in many cases, in Allhoff’s position it cannot be ruled out, and, in exceptional cases, it can be the lesser of two evils. Allhoff qualifies his position, by cautioning that “we must be extremely careful in choosing whether to utilize torture, paying close attention to our epistemic situations and our ability to constrain the use of torture to appropriate cases. These challenges are serious, but not insurmountable.” Readers interested in the current state of interrogational torture—as well as a cogent argument for the use of torture in limited circumstances—would be well advised to read this book.

