JOURNAL ON
TERRORISM & SECURITY
ANALYSIS

SPRING 2011

SATSA STUDENT ASSOCIATION on TERRORISM and SECURITY ANALYSIS

INSCT
INSTITUTE FOR NATIONAL SECURITY AND COUNTERTERRORISM
SYRACUSE UNIVERSITY

Journal on Terrorism and Security Analysis

Volume 6 • Spring 2011

Editorial Team

Table of Contents:

Dear Reader:

It is with great pleasure to introduce you to the 6th volume of the Journal on Terrorism and Security Analysis (JTSA). The editorial staff consists of graduate students from the Syracuse University College of Law, the Maxwell School and the Newhouse School of Public Communication. While JTSA's editors have various backgrounds and interests, the team shares a passion for national and international security.

Our journal acted as a clearing house for the Student Association on Terrorism and Security Analysis' (SATSA) annual conference. SATSA invited the authors producing the most comprehensive and thought provoking papers to present their findings. The keynote speaker was General Richard O'Meara; his article argues that scholars and strategists overemphasize the justification and means to wage war at the expense of discussing when a war is over. The discussion panel consisted of Braden Civins, Professor Jack Jarmon and Captain Sean Atkins. The panelists drew from their diverse background (law student, university faculty member and Air Force officer, respectively) to discuss relevant topics on crime and terrorism. Civins critiques the executive and legislative response to the Christmas "underwear bomber" in 2009, Jarmon discusses the role of cyber security and cyber terrorism and its implications and Atkins discusses similarities shared between violent non-state actors such as terrorists and street gangs.

This edition has a variety of authors and viewpoints; at times these views conflict with one another. While the journal is security focused, JTSA does not subscribe to an overarching ideology or worldview. Instead, we focus on promoting knowledge and critical thinking on the most salient security issues around the world. Our call for papers attracted submissions not just from various universities in the United States but from around the world. This is a testament to how national and international security is becoming increasingly blurred with a globalized economy and an ever "flattening" world. As Nyambura outlines in his article, terrorist attacks and government responses in Kenya and Ethiopia are not merely an African problem, but also have implications for the United States. Professor Mylonaki details how the American led "war on terror" has had spillover effects in the United Kingdom. She outlines how the counterterrorism legal regime in the UK challenges traditional human rights enjoyed by British subjects and residents. But the journal also promotes local talent: Nellywn Olson, from the Maxwell School of Syracuse University, questions the default view that North Korea is pursuing a nuclear weapons program by analyzing a report produced from a leading American nuclear scientest. Also, Brendan Noto from the University of Albany and a Navy veteran critiques American anti-piracy operations off the coast of Somalia.

National and international security is never static or purely academic. As this issue goes to print, world events implore policy makers to continually think outside the box. The international community is intervening with air strikes in Libya and revolutions are rocking Tunisia and Egypt. There are signs that Yemen, under the leadership of Ali Abdullah Saleh, is under extreme pressure to reform. Mayborn argues that US drone use in Yemen may cause potential backlash from the Yemeni population. Specifically, the Yemeni population may link cooperation between the Yemeni and American government on the use of armed UAVs in Yemen as American complicity with Yemeni repression and poor economic policy.

Finally, the editorial board is excited to put these articles on the web for academics, practitioners and students alike to utilize in the future. The editorial board would like to thank the Institute for National Security and Counterterrorism (INSCT) for the financial and moral support they provided for the project.

We hope you enjoy this years' issue.

Sincerely,
JTSA Editorial Board

AUTHOR BIOS

Christian Geib is pursuing a LLM at Stanford Law School. He earned his degree of Bachelor of Law LL.B. (J.D.equivalent) in 2006 as part of a multilingual/multijurisdictional degree of the Hanse Law School Program between the Universities of Bremen, Oldenburg (Germany) and Groningen (The Netherlands). Prior to his law school studies he had studied political science at the University of Tübingen (Germany) and the Catholic University of Santiago de Chile. During his studies he interned at the German Parliament, the international law department of the German Ministry of Defense and in corporate investment banking of *Deutsche Bank*. Following his graduation he worked with a large retail company and for a science and research policy project of the European Commission. Geib is a reserve officer with the German Armed Forces.

Braden Civins, a native Texan, is in his final year of study at The University of Texas, pursuing a J.D. from the School of Law and a Master of Global Policy Studies and specializing in Security Studies at the Lydon B. Johnson School of Public Affairs. He is a member of the Texas International Law Journal and former participant in the National Security Clinic, where he co-authored a successful appellate brief on behalf of a Guantanamo Bay detainee. He works at the Robert S. Strauss Center for International Security and Law. He spent recent summers working at the Criminal Prosecutions Division of the Texas Attorney General's Office, the House of Representatives Committee on Foreign Affairs, and the Department of State.

Richard M. O'Meara is a retired Brigadier General (USA) and trial attorney who teaches human rights, security issues, and international law in the Division of Global Affairs, Rutgers University. His is also developing a program of study leading to an Associate's Degree in Homeland Security Studies at Ocean County College, NJ. He has served as a resident fellow at the Stockdale Center for Ethical Leadership, US Naval Academy and has taught governance and rule of law issues in such diverse locations as Cambodia, Rwanda, Chad, Philippines, Guinea, Sierra Leone, Slovenia, Moldova, Ukraine, Bosnia-Herzegovina, Peru, El Salvador and Iraq. He served as an EMT for the Red Cross in following the 9/11 attack at the World Trade Center.

Nellwyn Olson is currently a Master of Arts candidate in International Relations at the Maxwell School of Citizenship and Public Affairs, where she is focusing on Global Security and East Asia foreign policy. Her research interests include identifying the illicit flow of nuclear materials in East Asia and the smuggling routes of drugs and weapons throughout Southeast Asia and Oceania. She graduated with a Bachelors in Business Administration from the Stephen M. Ross School of Business at the University of Michigan where she studied corporate strategy, Southeast Asian area studies, and economics.

Sean Atkins is an active duty officer in the United States Air Force. He has deployed to both Iraq and Afghanistan, where some of the ideas presented in this article first took shape. He holds a BA with honors from the University of Southern California and an MA with distinction from King's College London.

Dr. Emmanouela Mylonaki is a Senior Lecturer in Law at London South Bank University, UK and Director of Postgraduate Studies. Mylonaki holds an LLB from the University of Athens, an LLM in International Law University of Westminster, an MPhil in Criminology from Cambridge and a PhD in Law from Bristol University. Her academic research focuses broadly on international criminal law and more specifically on international terrorism and counter-terrorism legislation.

Tim Burton is a Crown Prosecutor currently working in London. He holds an LLB degree and an LLM in Crime and Litigation from London South Bank University. He is a guest lecturer on terrorism and policing at London South Bank University.

Brendon Noto graduated from the University at Albany with a BA in European History and American Politics. He is pursuing his MA in International, Global and Comparative History at the University at Albany. His subjects of interest include naval policy and post-Cold War International Relations. Brendon Noto served in the U.S. Navy and conducted anti-piracy and Visit Board Search and Seizure operations off the coast of Somalia over the course of two deployments.

William Mayborn is from Dallas, Texas, and received his bachelor's degree in Asian Studies and History from the University of Texas at Austin. William spent a considerable amount of time in China studying Chinese, teaching English, and pursuing business ventures. He is now currently pursuing his master's degree at the Bush School of Government and Public Service at Texas A&M University in College Station. His security study interests are in counter-terrorism, counter-insurgency, Afghan military issues, and Chinese security issues.

Jack Jarmon is the Associate Director of the Command Control and Interoperability Center for Advance Data Analysis at Rutgers University, an adjunct Professor at Seton Hall University and the Chief Research Officer at the New Era Associates. From 2008-2009 he was a lecturer at University of Pennsylvania. He was a technical advisor to USAID in the South Russian Privatization Center. Jarmon got his BA from Rutgers University, an MA from Fordham University and a PhD from Rutgers University. His published piece is one chapter from an upcoming textbook on security studies and international relations.

Simon Nyambura is a doctoral candidate in Security Studies at Kansas State University. He earned an M.A. in international Studies at the University of Nairobi, Kenya, and received a B.A. cum laude from the University of Nairobi. Nyambura has worked as a political and security analyst and consultant for several non-governmental organizations in the Horn of Africa. His research interests include security, conflict, peace and politics in Africa. He is Kenyan.

Salient but Unappreciated: Issues in National and International Security and Defense Policy for the Next Decade

Christian Geib

The author would like the following persons: Thomas Schafbuch and the whole editorial team on the Journal on Terrorism and Security Analysis for their tireless support and patient editing, my fellow LL.M. student Moran Druker at Stanford Law School for her suggestions and research concerning the "Iron Dome" and Professor Drury Stevenson of the University of South Texas College of Law for directing my attention to the "Black Swan" and insurance considerations through his intriguing presentation at the Defense Policy Symposium at Stanford on Jan. 22, 2011 and his inspiring article, The Effect of National Security on the Criminal Law Paradigm.

1. The Neglected Issues of Combined Arms -the Hubris of Predicting Future Warfare:

As much as scholars of all academic disciplines would like to think of their discipline as purely based on observation and analysis, undoubtedly they are subject to temporary fashion cycles which influence the debate beyond mere scientific findings and scientific reasoning.

Military strategy and defense policy are no exception to that. Throughout military history, military thinkers have been subject to such cycles with concerns to the question of what really was at the contemporary *cutting edge* nature of warfare and what the future of warfare would be like.

As most prominently articulated in the "Rumsfeld Doctrine[1]" with its emphasis on ever lighter, Special Forces-focused *Blitzkrieg* approach, currently to most defense policy planners and scholars it appears that *counterinsurgency*[2] (COIN) or *counterterrorism* are "the only games in town" for future military campaigns. Large Cold War-like ground forces are synonyms for being *obsolete* in modern defense policy and portrayed as being, once and for all, a phenomenon of the past.

Instead, the future seems to be entirely dominated by *asymmetric warfare*, i.e. warfare with severe imbalances of strength between the combating parties.[3] Part of this apparently inevitable asymmetrical future combat scenario is to be the so called *"Three Block Warfare."*[4] The concept of the "three-block war" was promulgated by Marine Corps General Charles Krulak.[5] Krulak realized that on the modern battlefield, Marines could be called upon to perform very different missions simultaneously. On one block they might be engaged in high-intensity combat, on the next block they might be handing out relief supplies and on the third block they might be separating warring factions.[6]

Small, light, modern, highly expeditionary forces for swift peacekeeping, peace enforcement, evacuation, counterterrorism or counterinsurgency missions appear to be the military strategy consensus amongst most major European NATO powers, such as England, France and Germany, who have recently agreed on substantial cuts and restructuring of their military in sheer numbers and "heavy" equipment.[7]

---

[1] Carl Robichaud, *Failings of the Rumsfeld doctrine-Intense air power and small groups of troops didn't win in Iraq or Afghanistan (*September 21, 2006), http://www.csmonitor.com/2006/0921/p09s02-coop.html (last visited Dec. 31, 2010); Michael E. O'Hanlon, *A Reality Check for the Rumsfeld Doctrine*, (APRIL 29, 2003); http://www.brookings.edu/opinions/2003/0429defense_ohanlon.aspx , (last visited Dec. 31, 2010).

[2] Especially following the widely acclaimed work of one of the leading scholars in this field, David Kilcullen and his most recent publications: DAVID KILCULLEN, THE ACCIDENTAL GUERRILLA: FIGHTING SMALL WARS IN THE MIDST OF A BIG ONE (2006); DAVID KILCULLEN, COUNTERINSURGENCY (2010).

[3] Id. At 22: "In mid-2008 supplemental budget allocation for the Iraq war the , the US defense budget is approaching 70 percent of the global defense spending which is bound to make any military engagement of the United States against another party highly asymmetrical; Richard Norton-Taylor, *Asymmetric warfare Military planners are only beginning to grasp the implications of September 11 for future deterrence strategy,* THE GUARDIAN, (from October 3, 2001), http://www.guardian.co.uk/world/2001/oct/03/afghanistan.socialsciences (last visited Feb. 7, 2011); Toni Pfanner, *Asymmetrical Warfare from the Perspective of Humanitarian Law and Humanitarian Action,* Vol. 87 No. 857 (March 2005), https://docs.google.com/viewer?url=http://www.icrc.org/eng/assets/files/other/irrc_857_pfanner.pdf (last visited on Feb. 7, 2011): "The fundamental aim of asymmetrical warfare is to find a way round the adversary's military strength by discovering and exploiting, in the extreme, its weaknesses. Weaker parties have realized that, particularly in modern societies, to strike "soft targets" causes the greatest damage. Consequently, civilian targets frequently replace military ones... The term "symmetrical warfare" is generally understood to mean classic armed conflict between States of roughly equal military strength.7 The wars that took place in the eighteenth and nineteenth centuries — i.e. after the Peace of Westphalia — in which evenly matched government troops confronted and fought each other in open battles have sometimes been called a thing of the past, for in the twentieth century wars became more complex and more unequal. Furthermore, most wars nowadays are internal, although they frequently have international ramifications. They are as diverse as they are numerous and the way in which they are conducted varies according to the type of conflict…" (at 151-52).

[4] Also referred to as Fourth-Generation Warfare, see: Tony Corn, *World War IV was Fourth-Generation Warfare,* HOOVER INSTITUTION STANFORD UNIVERSITY POLICY REVIEW JAN. 2006, http://www.hoover.org/publications/policy-review/article/6526 (last visited Feb. 8, 2011).

[5] Max Boot & Jeane J. Kirkpatrick, *Beyond the 3-block war*, ARMED FORCES JOURNAL in: Council of Foreign Relations (March 2006), http://www.cfr.org/united-states/beyond-3-block-war/p10204?breadcrumb=/publication/publication_list%3Ftype%3Djournal_article%26page%3D10 (last visited Feb. 7, 2011).

[6] Id.

[7] *Germany's Responsible Military Reform,* The New York Times, December 29, 2010, at A 28; *Military Reform: Conscription in*

However, when such theories like the "Rumsfeld Doctrine" were put to the test during operation *Iraqi Freedom* in 2003, the lack of sufficient "boots on the ground" in itself posed a problem with stabilizing Iraq immediately after major combat operations had ended in 2003.

Already during the initial "shock and awe" phase of the 2003 Iraq campaign it became apparent that the great strength of the "outdated" old, heavy armor lay in its great robustness. On a number of occasions, even in situations of being heavily outnumbered, during operation *Iraqi Freedom* the M1 Abrams tanks stood their ground in situations where lighter and more *modern* Striker Brigades would have suffered substantial numbers of casualties.[8]

German troops in Afghanistan had shown that unexpectedly it was not the swiftly moving "modern" light infantry that dominated the fierce fighting in their sector, but the old-fashioned, Cold War-like, slow moving armored infantry, the *Panzergrenadiers.*[9] This was illustrated by a number of fierce firefights with insurgents in the Northern Province of Kunduz.

In one firefight a platoon of German Army paratroopers was ambushed during a foot patrol on April 2, 2010 in the village of Isa Khel.[10] During this firefight the German platoon was outgunned and outnumbered. The German paratroopers and the supporting armored vehicles were only equipped with assault rifles of 5.56 mm caliber and machine guns of 7.62 mm caliber. The insurgents made use of strategically positioned improvised explosive devices (IED) (which destroyed one of the vehicles trying to evacuate some of the wounded soldiers), AK-47 assault rifles, heavy machine guns, rocket propelled grenades (RPG) and mortars. Due to the vicinity of populated areas and scarcity of combat helicopters in this Province of Afghanistan, air support (other than for mere show of force) could not be

---

Germany to End Next Summer, DER SPIEGEL, Nov 23, 2010, http://www.spiegel.de/international/germany/0,1518,730660,00.html (last visited Dec. 31,2010); *In Retreat German Military Reform Could Halve Ground Forces,* DER SPIEGEL, Aug. 9,2010, http://www.spiegel.de/international/germany/0,1518,710853,00.html, (last visited Dec. 31, 2010); Robin Bravender, *European countries downsize military, increase social programs,* (October 30, 2006), http://www.theeagleonline.com/news/story/european-countries-downsize-military-increase-social-programs/ (last visited Dec. 31, 2010); *SAS cuts raise concerns over UK's military strength,* (September 16, 2010), http://rt.com/news/sas-downsize-budget-slash/; (last visited Dec. 31, 2010); James Kirkup, *Defense spending: thousands of troops to be cut* (Sep 10, 2010), http://www.telegraph.co.uk/news/newstopics/politics/defence/7995646/Defence-spending-thousands-of-troops-to-be-cut.html (last visited Dec. 31, 2010); DAVID STRINGER, *British Armed Forces Cuts Announced: UK Addresses Deficit, Trims Defense Spending* (Oct. 19,2010), http://www.huffingtonpost.com/2010/10/20/royal-armed-forces-cuts-a_n_769446.html, (last visited Dec. 31, 2010); *U.K. Defense Spending Cuts Worry Clinton*, CBS News (Oct. 15, 2010), http://www.cbsnews.com/stories/2010/10/15/world/main6960705.shtml (last visited Dec. 31, 2010); Henry Chu Los Angeles Times, *European allies to slash military spending While officials point to big budget deficits, critics say they will cede their role on the world stage* (Dec. 26, 2010), http://www.philly.com/inquirer/world_us/20101226_European_allies_to_slash_military_spending.html (last visited Dec. 31, 2010); Pierre Tran , *France To Cut Spending $4.8B Over 3 Years* (Sep 28, 2010), http://www.defensenews.com/story.php?i=4799913 (last visited Dec. 31, 2010*); Germany - Military Spending,* GlobalSecurity.Org, (July 2010), http://www.globalsecurity.org/military/world/europe/de-budget.htm (last visited Dec 31, 2010); Spencer Ackerman, *Deficit Plan Scraps Pentagon Jets, Tanks, Trucks*, (November 10, 2010), http://www.wired.com/dangerroom/2010/11/deficit-plan-scraps-pentagon-jets-tanks-trucks/ (last visited Dec. 31, 2010); Hans Binnendijk et. al, *Defense Cuts: A Rescue Plan for NATO* (November 4, 2010), http://www.atlantic-community.org/index/articles/view/Defense_Cuts:_A_Rescue_Plan_for_NATO_ (last visited December 31, 2010); *Budget Cuts Are a Good Pretext for Reforming Military Policy*, DEFENCE TALK (SEPTEMBER 8, 2010), http://www.defencetalk.com/budget-cuts-are-a-good-pretext-for-reforming-military-policy-28597/ (last visited December 31, 2010).; Quentin Peel and James Blitz, *Security: A German military overhaul,* FINANCIAL TIMES FT.COM (Published: January 31 2011 09:07 pm Last updated: January 31 2011 09:07 pm), http://www.ft.com/cms/s/0/c0fedfdc-2d6f-11e0-8f53-00144feab49a.html#axzz1DYuBNyBv (last visited Feb.9, 2010); *New model army,* FINANCIAL TIMES FT.COM, Published: November 18, 2010 10:55 pm, Last updated: November 18, 2010 10:55pm) http://www.ft.com/cms/s/0/9253fe06-f35e-11df-b34f-00144feab49a.html#axzz1DYuBNyBv (last visited Feb. 9, 2011):

> …Modernization was overdue. During the cold war, the German army's role was to act as a speed-bump for Soviet tanks dashing westwards. Times and threats have changed. But Germany maintains its static defensive posture. Although its army is one of the largest in Europe, its ability to deploy forces overseas is minimal… A professional army with greater expeditionary capacity will allow Germany to shoulder a greater burden in international operations. With pan-European defense cuts making inroads into the capacity of organizations such as NATO, this would be a positive development…

> During the Cold War, the German army's role was to act as a speed-bump for Soviet tanks dashing westwards. Times and threats have changed. But Germany maintains its static defensive posture. Although its army is one of the largest in Europe, its ability to deploy forces overseas is minimal…
>
> A professional army with greater expeditionary capacity will allow Germany to shoulder a greater burden in international operations. With pan-European defense cuts making inroads into the capacity of organizations such as NATO, this would be a positive development…

[8] David Talbot, *How Technology Failed in Iraq* (NOVEMBER 2004), http://www.technologyreview.com/computing/13893/ (last visited Dec. 31, 2010); Frank Lewis, *Iraq War veteran speaks about experiences in Baghdad*, (Nov. 1, 2010), http://www.portsmouth-dailytimes.com/view/full_story/9942416/article-Iraq-War-veteran-speaks-about-experiences-in-Baghdad?instance=home_news_lead (last visited Dec. 31, 2010);

[9] *Schützenpanzer Marder: Das 20-Millimeter-Argument*, German Army Homepage (July 16, 2010), http://www.bundeswehr.de/portal/a/bwde/einsaetze/missionen/isaf?yw_contentURL=/C1256EF4002AED30/W287EAH5365INFODE/content.jsp (last visited Dec 31, 2010).

[10] Id.

deployed. Therefore, it took the German platoon and the reinforcements a several hour-long firefight to pull out of the area. During the firefight it became apparent that the 5.56 mm and 7.62 mm bullets of the German soldiers were not able to penetrate the thick clay walls of the surrounding buildings. Thus, the German paratroopers were not able to eliminate many emplacements of the insurgents. However, in return the insurgents with their RPGs *were* able to target German soldiers seeking cover behind the very same clay walls. In total 3 German soldiers were killed and 8 wounded.[11]

Moreover, a poorly marked vehicle of the Afghan National Army (ANA) that was rushing to the help of the German forces was targeted by German reinforcement troops as it approached them with high velocity. During this "friendly fire" incident 5 ANA soldiers were killed.[12]

Following this fierce firefight the German Minister of Defense zu Guttenberg ordered that the number of the available heavily armored infantry combat vehicle *Marder* for the German contingent be doubled. The *Marder* 1 A3 vehicle had originally been introduced into the German Armed Forces in the 1970s and developed for Cold War scenarios of large tank and infantry battles. With the end of the Cold War most military strategists viewed the *Marder* and the whole concept of heavily armored infantry as obsolete and inapt to adapt to modern challenges.[13]

However, this seemingly "obsolete" 38 metric ton *Cold War* vehicle with its 20mm canon soon proved its usefulness in the Northern Afghan Provinces once the German Army had taken over the responsibility of the *Quick Reaction Force* in the Northern ISAF sector.[14]

The *Marder* especially showed its usefulness during the fierce engagement at July 19, 2009 at Zar-Kharid-i-Sufla nearby Kunduz[15]:

A German *Panzergrenadier*-Platoon managed to rescue a unit of the Afghan National Army (ANA) that was accompanied by Belgian military advisers and had come under heavy fire from insurgents. The 20mm canon managed to eliminate insurgent emplacements behind thick stone and clay walls which rapidly ended insurgent resistance during this firefight.[16]

This constituted the kind of firepower and armor that was sorely missed during the engagement at Isa Khel.

As a lesson learned of the tragic firefight at Isa Khel, the German Army also changed the training of its light infantry units. Future contingents of paratroopers were trained in heavy, armored infantry tactics and cooperating with *Panzergrenadiers* before their deployment.[17] Such training before was solely limited to the *Panzergrenadiers*.

In the aftermath of Isa Khel the German Minster of Defense zu Guttenberg ordered three heavily armored self-propelled artillery guns, the *Panzerhowitzer 2000* to be deployed immediately to Kunduz province.[18] In 2011 he ordered a further two of these gigantic self-propelled guns as a reserve to Kunduz province. Even though considered one of the currently most advanced artillery systems worldwide, the *Panzerhowitzer 2000* was originally designed for the Cold War battlefields. With its maximum weight of 56 metric tons it defies current doctrines of light and highly expeditionary forces.[19] Undoubtedly the deployment of this massive Cold War artillery has shown the limits and difficulties of such "old" heavy armor, as one entire gigantic Russian *Antonov 124-100* airplane was necessary for just two such artillery systems.[20] Nonetheless, this piece of seemingly outdated Cold War equipment has proved its value for the ISAF troops in Kunduz province. Support with highly explosive grenades, exercise grenades (with limited explosive effect, e.g. if proximity to civilian areas makes the use of regular explosive ammunition too risky) fog screens and illumination projectiles[21] proved to be immensely beneficial support to the local ISAF forces.[22] This support was delivered substantially faster

[11] Id.
[12] *Afghan soldiers killed in friendly fire*, (from April 03, 2010), http://articles.cnn.com/2010-04-03/world/afghanistan.friendly.fire_1_gen-eric-tremblay-afghan-defense-ministry-german-troops?_s=PM:WORLD (last visited on Feb. 5, 2011).
[13] Id.
[14] *Germany Takes Over Quick Reaction Force in Afghanistan* (from June 30, 2008), http://www.dw-world.de/dw/article/0,,3451110,00.html (last visited Feb 6, 2011).
[15] *Schützenpanzer Marder: Das 20-Millimeter-Argument*, German Army Homepage (July 16, 2010), http://www.bundeswehr.de/portal/a/bwde/einsaetze/missionen/isaf?yw_contentURL=/C1256EF4002AED30/W287EAH5365INFODE/content.jsp (last visited Dec 31, 2010).
[16] Id.
[17] Id.
[18] *Truppenbesuch im Norden des Landes: Guttenberg will Truppe in Afghanistan besser ausstatten (*from April 14, 2010), http://www.tagesschau.de/ausland/guttenbergafghanistan102.html (last visited Feb. 7, 2011);
[19] *Panzerhaubitze 2000* (homepage of the German army with the basic technical data without providing any specific date of the contribution), http://www.deutschesheer.de/portal/a/heer/!ut/p/c4/NYvLCsIwEEX_aCYNSIuuFBFEqEttd2k6tEObB2GqIH68ycJ74GwOF3vMePPiyQgHb1Z8Ymd5P7xhJkogZGfPCywkQjCbbWD5kFZK4aNcjYuHkcAGT1Is5IWzp2QkJIghyVrKllluwCN2qjqf1E79V33rum_am9bNtb3cMTp3_AHdZdGo/ (last visited Feb. 7, 2011).
[20] *Eiserne Reserve für Kunduz*, (from Jan. 28, 2011); http://www.deutschesheer.de/portal/a/heer/!ut/p/c4/NYzBCsIwEET_aDcRiuLNUAU96FHrbU1DE5smZdnoxY83FZyB4cEMg3esTvQKA0nIiSLesLNh-3iDd46BRikuRkhkPQfrxSV4kueV0rpCKvRDvC4_vQObk5Ml61BCzYFJMsOcWeLSFObaQOixU7o1qIF_6c-mPe2NWTfqeD5ccJ6m3RegFaEg/ (last visited on Feb. 7, 2011): the article describes the deployment of two additional reserve artillery pieces to Kunduz province in addition to the three already stationed there.
[21] *Team und Technik der Panzerhaubitze* (from July 23, 2010), http://www.bundeswehr.de/portal/a/bwde/einsaetze/missionen/isaf?yw_contentURL=/C1256EF4002AED30/W287LJGW809INFODE/content.jsp.html (last visited Feb. 7, 2011): this article described the technology of the artillery piece and the different sorts and uses of ammunition.
[22] *Afghanistan: Einsatz der Panzerhaubitze 2000* (from Aug. 5, 2010), http://www.bundeswehr.de/portal/a/bwde/einsaetze/missionen/isaf?yw_contentURL=/C1256EF4002AED30/W28829RC123INFODE/content.jsp.html (last visited on Feb.6, 2011): this article described the support of American ISAF forces by illumination rounds by the *Panzerhowitzer 2000*; *Afghanistan: Panzerhaubitze gegen gegnerische Kräfte eingesetzt* (from Nov.

(and considerably cheaper) than any close air support (CAS).

Another interesting comeback with the German armed forces was that of the old Cold War assault rifle HK G-3 which had already been replaced by the more modern HK G36 rifle. However, as the "old" HK G-3 assault rifle with its 7.62 mm caliber showed a far greater penetration power than the modern (and considerably more precise) modern HK G-36 (made mostly of carbon composite materials and advanced sights) with its 5.56 mm caliber. Therefore, the German ISAF contingent currently uses a mix of both assault rifles for its infantry units.[23]

The latest large scale Lebanon Campaign of the Israel Defense Forces (IDF) showed[24], that even an Army that has been honing its *counterinsurgency* and *counterterrorism* skills since the last full scale Israeli-Arab conflict in 1973, suddenly can be put in a situation of using more "old fashioned" large scale operations. Moreover, the conduct of the Lebanon campaign showed that after years of practicing solely *counterinsurgency* and *counterterrorism,* crucial military *core business* skills such as the combined arms warfare (the cooperation of the various branches of the army such as infantry, artillery, tanks etc.) are substantially weakened if neglected.[25] Losing such core capabilities can prove to be disastrous for any army committing the fallacy of presuming that present day warfare is the only type of warfare for future conflicts.

Thus, it is imperative to any security and defense policy to prepare for both: the kind of warfare the strategic establishment assumes (or desires) to be the likely future scenario *and* those scenarios found to be "unlikely" at present.

2. Developed country's demographics and obesity as a risk to national security-A return to the draft in the foreseeable future?

An issue less frequently referred to as a risk to national security is the issue of demographics and the epidemic of child and adolescent obesity.

Germany was the last of Western Europe's major powers to announce the abolishment of the draft/mandatory military service for June 2011.[26] Think tanks such as Stanford based *Center for International Security and Cooperation* (CISAC) are rather quick to conclude that at present such a draft would neither be politically feasible nor would a resulting large scale army be needed.[27] This, however, says little about the foreseeable future when an increasingly aging population, especially in Europe, might again necessitate such a draft – provided that societies do not want to resort to overt mercenary armies largely composed of foreigners or even larger involvement of private military firms (PMF).[28]

An increasingly recognized issue for national security is the vastly increasing percentage of obesity amongst children and young adults, which has become

---

1, 2010), http://www.bundeswehr.de/portal/a/bwde/einsaetze/missionen/isaf?yw_contentURL=/C1256EF4002AED30/W28ASHXK951INFODE/content.jsp.html (last visited on Feb. 6, 2011): this article describe the use of the *Panzerhowitzer 2000* in the support of ISAF forces;

[23] Stephan Löwenstein, *Mit großem Kaliber gegen die Taliban*, (from July 12, 2010), http://m.faz.net/RubDDBDABB9457A437BAA85A49C26FB23A0/Doc~E25ADC365E957456A99044E4C979A918A~ATpl~Epartner~Ssevenval~Scontent.xml (last visited on Feb. 7, 2011).

[24] David E. Johnson, *Military Capabilities for Hybrid War Insights from the Israel Defense Forces in Lebanon and Gaza*, RAND Corporation Occasional Papers (2010) at 2-3:

> The Israelis were very successful at LIC in the years before the Second Lebanon War, suppressing the intifada and dramatically lowering Israeli casualties. Unfortunately for Israel, as operations in Lebanon in 2006 would show, the Israeli Army's almost exclusive focus on LIC resulted in a military that was largely incapable of joint combined arms fire and maneuver… Eventually, Israeli ground forces entered Lebanon, where they had real difficulties, well documented in Matt Matthews's *We Were Caught Unprepared*… defeating Hezbollah required joint combined arms fire and maneuver, something the IDF was largely incapable of executing in 2006. Fire suppresses and fixes the enemy and enables ground maneuvering forces to close with him. Fire also isolates the enemy, shutting off lines of supply and communication and limiting his ability to mass. Maneuver forces enemy reaction. If the enemy attempts to relocate to more favorable terrain, he becomes visible and vulnerable to fire. If he remains in his positions and is suppressed, he can be defeated in detail by ground maneuver. Thus, hybrid opponents like Hezbollah demand integrated joint airground-ISR capabilities that are similar to those used against conventional adversaries, but at a reduced scale. Finally, the IDF's highly centralized C2 system, which had been effective in confronting the intifada, proved problematic against Hezbollah…

[25] Which in German military doctrine is called fittingly "Gefecht der verbundenen Waffen", i.e. "the combat of connected /joined weapons").

[26] *Military Reform: Conscription in Germany to End Next Summer,* DER SPIEGEL, Nov 23, 2010, http://www.spiegel.de/international/germany/0,1518,730660,00.html (last visited Dec. 31, 2010).

[27] See discussion hosted by CISAC at Stanford from Dec. 7, 2010, recorded under http://cisac.stanford.edu/news/the_ethics_of_the_draft_20101207/ (last visited Dec. 31, 2010); This fear of a large scale army neglects the possibility of a lottery system draft which would at least potentially make the entire military aged population liable to military service.

[28] To be sure, Europe and the whole developed (Western) World is not alone with the problem of aging societies as China's estimated fertility rate per woman is 1.6 children, well below the 2.1 needed to keep a population stable, and there may be other factors reining in China's population. Some predict that up to 30 million Chinese men won't have brides available to them by 2020 because the policy spurred selective abortion of girls. Others worry about the economic effect the policy will have, given an aging population. However, given the sheer size of the Chinese population this should still not lead to a server shortage of military aged men and women, see: Dan Murphy, *Suicide attacks down, Predator drone exits, and other overlooked stories in 2010* (Dec 22, 2010), http://www.csmonitor.com/World/Global-Issues/2010/1222/Suicide-attacks-down-Predator-drone-exits-and-other-overlooked-stories-in-2010 (last visited January 6, 2010).

the leading reason for the medical rejection of recruits. It is currently estimated that more than a quarter of all Americans aged 17 to 24 were unfit for service due to obesity.[29]

This constitutes a multi-facetted challenge for libertarian societies where mandatory exercising and banning of certain food items is not an option. Assuming educative campaigns are successful; this problem will endure for a substantial period of time.

A further demographic challenge to many developed (especially Western) societies is the difficulty to recruit the brightest university graduates for a career in the armed forces, especially in areas like computer science, which offer high-paying civilian career perspectives.[30] Especially for Western countries which are already burdened by a general aging and shrinking (military age) population this serious recruitment challenge is concerning. This problem is further aggravated in the context of non-Western countries with very developed cyber-warfare capacities, such as China, being able ensure through conscription that their brightest computer science students are at least temporarily contributing to their military's cyber-warfare capacities rather than joining high-paying jobs with companies such as *Google* or *Facebook* directly after leaving university.[31]

With the cyber-warfare arms race already having started, particularly by states that are disadvantaged in their conventional warfare capacity, the cyber-warfare capability of Western countries might crucially depend on enrolling some of its brightest minds in computer science either through conscription or through substantive, likely financial, incentives currently not available for military service.

---

[29] Alex Spillius in Washington, *Obesity among US schoolchildren 'a risk to national security'* (Apr. 25, 2010), http://www.telegraph.co.uk/news/worldnews/northamerica/usa/7632462/Obesity-among-US-schoolchildren-a-risk-to-national-security.html (last visited Dec. 31, 2010)

[30] Kevin Poulsen, *Air Force Launches Recruitment Campaign Touting Cyber Command*, (from Feb. 27, 2008), http://www.wired.com/threatlevel/2008/02/air-force-launc/ , (last visited on Feb. 5, 2011); Keith Epstein/Brian Grow, *Recruiting for the Cyber Wars Uncle Sam wants you—to help defend against Internet threats. But is the military any place for slackers and hackers?* (from April 15, 2008), http://www.businessweek.com/bwdaily/dnflash/content/apr2008/db20080414_422082.htm (last visited on Feb. 5, 2011); Tim Kane, *Why Our Best Officers Are Leaving*, The Atlantic, Jan./Feb.2011, http://www.theatlantic.com/magazine/archive/2011/01/why-our-best-officers-are-leaving/8346/1/ (last visited on Feb. 5, 2011); additionally in the popular surveys addressing the "best places where to start a career" it would be rather difficult to see the military mentioned among the top 100 ranks (when even Teach for America is mentioned there as one of the few NGO/Government Jobs), see e.g.:
Best Places to Launch a Career 2008 by Business Week, http://www.businessweek.com/interactive_reports/career_launch_2008.html , (last visited Feb. 5, 2011); *Best Places to Launch a Career 2009* by Business Week, http://www.businessweek.com/interactive_reports/career_launch_2009.html, (last visited on Feb. 5, 2011).

[31] *PLAN Conscripts Conscription Process*, http://www.globalsecurity.org/military/world/china/plan-personel-enlistedforces-conscripts.htm (last visited January 6, 2011); an interesting advertisement of the story of a Chinese student returning from his studies in Canada to join the Chinese armed forces can be found on an English speaking webpage apparently affiliated with the Chinese Army: *Wang Feilin's conscription story* (2010-Jan 12, 2010, 8:58 pm), http://www.chnarmy.com/html/2010-12/8384.html (last visited January 6, 2011); John Markoff et al., *2 China Schools Said to Be Tied to Online Attacks,* NY TIMES (February 18, 2010), http://www.nytimes.com/2010/02/19/technology/19china.html (last visited January 6, 2011); *Chinese army must deal with cyberwarfare: state media*, http://www.physorg.com/news/2010-12-chinese-army-cyberwarfare-state-media.html (last visited January 6, 2011); *CYBER WARFARE Risking chaos in the sky,* http://www.propilotmag.com/archives/2010/Apr%2010/A2_Cyberwarfare_p3.html (last visited January 6, 2011); *Chinese army to recruit university students*, http://www.study-in-china.org/ChinaEducation/PolicyLaws/20091112128115129.htm (last visited January 6, 2011); The "Active-Duty Officer's Law" and the "Regulations on the Appointment and Dismissal of Officers in Active Service" provide for standard performance appraisal based on evaluations by senior officers, a unit's political officer, and officer peer reviews. In some cases, evaluations combine such appraisals with objective examinations on subjects ranging from military technology to foreign languages to computer science, see: THE "PEOPLE" IN THE PLA: RECRUITMENT, TRAINING, AND EDUCATION IN CHINA'S MILITARY, (Roy Kamphausen et al. eds., Strategic Studies Institute, at 10, U.S. Army War College, 2008); Id. at 33: "…most of the PLA's educational institutions now offering graduate courses.33 Other curriculum changes were introduced in 1987 with the Interim Regulations on academic work. One important change was to broaden the focus of technical classes to expose students to a wider range of topics, and greater efforts were made to combine technical and command training. In addition, new kinds of courses have been added to the curriculum of many military academies, including military education theory, military psychology, foreign policy, international relations, management, and computer programming…"; Id. 109-:… College Students Entering the PLA:...Since the turn of the century, the PLA has tried to attract more college educated people into its ranks, not only as officers but also as NCOs and conscripts. So far, the number of college students entering the military as privates is relatively small; According to a 2006 *Xinhua* report, "more than 10,000" college students have entered the Army in the 5 years this policy has been in effect.16 Nonetheless, this trend appears to be on the rise, as 2,850 undergraduates from 73 institutions of higher learning in Beijing alone were reported to have volunteered for the Army in 2006…; Id. 298: Curriculums: To educate the "new-type military talent," curriculums of the command colleges have also undergone major changes… courses on space operations, cyber-space operations, counterterrorism, military-operations-other-than-war, peacekeeping, and international law have also been added…; *US embassy cables: China uses access to Microsoft source code to help plot cyber warfare, US fears*, The Guardian, 4 December 2010, http://www.guardian.co.uk/world/us-embassy-cables-documents/214462?INTCMP=SRCH (last visited January 6, 2011); The emphasis on information warfare has forced the PLA to recruit from a wide swath of the civilian sector, according to the report. As is the case with the U.S. military and its new Cyber Command, the PLA looks to commercial industry and academia for people possessing the requisite specialized skills and pasty pallor to man the keyboards. And although it hints broadly at it, the report offers no evidence of ties between the PLA and China's hacker community, see: Mark Rutherford, *Congressional commission focuses on China's cyberwar capability* (Oct 22, 2009 5:03 PM), http://news.cnet.com/8301-13639_3-10381621-42.html (last visited January 6, 2011).

3. Not *Vietnamization, Iraqization,* or *Afghanization* as Western Exit Strategies but "Technologization"/"Mechanization":

Prior to the "*Surge*" in Iraq in 2007 "Iraqization"[32] was the new buzzword that was enthusiastically used by strategists trying to find a solution to the "quagmire"[33] of the very critical situation in Iraq.

Increasingly with all major European military announcing concrete or vague but certainly definite draw-down dates for their forces in Afghanistan the word of Afghanization[34] has surfaced, albeit not as prolifically used as the "Iraqization" or "Vietnamization"[35] of earlier times.

However, when revisiting the history of the involvement of the United States in Vietnam and of the Soviet Union in Afghanistan it becomes questionable if this strategy of a sudden draw-down/retreat of forces and propping up of unpopular governments and their often ill-trained and ill-disciplined local security forces could realistically result in stable countries able to defeat insurgencies or military incursions.[36]

Western societies are known for their casualty wariness. For example, casualty aversion was very consciously exploited during the genocide in Rwanda when Belgian soldiers were slaughtered by Hutu militias[37], a lesson well learned by the militias from the UN mission in Somalia when the death of 19 US Soldiers during the *Battle of Mogadishu*[38] prompted the U.S. and the other involved Western Countries to abandon the mission in Somalia and draw back their troops. This demonstrates that missions to provide assistance to governments and their security forces cannot be sustained indefinitely at a certain intensity of conflict.

---

[32] Larry Diamond/James Dobbins et al., *What to do in Iraq: A Roundtable,* FOREIGN AFFAIRS, July/August 2006, http://www.foreignaffairs.com/articles/61745/larry-diamond-james-dobbins-chaim-kaufmann-leslie-h-gelb-and-ste/what-to-do-in-iraq-a-roundtable (last visited on Feb. 5, 2011); *Iraq: The Way Forward—Assessing Iraqization* [Rush Transcript; Federal News Service, Inc.], COUNCIL ON FOREIGN RELATIONS, (from March 20, 2006), http://www.cfr.org/iraq/iraq-way-forwardassessing-iraqization-rush-transcript-federal-news-service-inc/p10216 (last visited Feb. 6, 2011); Stephen Biddle, *Seeing Bagdad, Thinking Saigon,* FOREIGN AFFAIRS, March/April 2006, http://www.foreignaffairs.com/articles/61502/stephen-biddle/seeing-baghdad-thinking-saigon (last visited Feb.6, 2011).

[33] Another, almost iconic word of the Vietnam era, enthusiastically used by American and foreign opponents of the wars in Iraq and Afghanistan alike: David Rudenstine, *Vietnam: 'Quagmire' Quackery*, THE NATION, March 5, 2001, web edition: http://www.thenation.com/article/vietnam-quagmire-quackery (last visited on Feb. 4, 2011); Jeffrey Record/Andrew Terril, *Iraq and Vietnam: Differences, Similarities, and Insights*, (from May 2004), http://www.strategicstudiesinstitute.army.mil/pubs/summary.cfm?q=377 (last visited Feb.3, 2011).

[34] Gilles Dorronsoro, FIXING A FAILED STRATEGY IN AFGHANISTAN, THE HUFFINGTON POST (from Nov. 18, 2009, 4:27 PM), http://www.huffingtonpost.com/gilles-dorronsoro/fixing-a-failed-strategy_b_362720.html (last visited Feb. 1, 2011).

[35] Robert H. Johnson, *Vietnamization: Can it work?,* FOREIGN AFFAIRS (from July 1970), http://www.foreignaffairs.com/articles/24176/robert-h-johnson/vietnamization-can-it-work (last visited on Feb. 5, 2010); *The World: What It Means For Vietnamization*, TIME Magazine (from Mon., Apr. 5, 1971), http://www.time.com/time/magazine/article/0,9171,876901,00.html (last visited on Feb. 4, 2011).

[36] Certainly when neither the security forces have achieved a sufficient level of training nor basic civil society institutions have been properly developed.

[37] A staggering, very personal account of the Rwandan Genocide and the slaughter of the Belgian soldiers can be found in the book by the former commanding general of the ill-fated United Nations Assistance Mission for Rwanda (UNAMIR): ROMÉO DALLAIRE, SHAKE HANDS WITH THE DEVIL: THE FAILURE OF HUMANITY IN RWANDA (2003) at p. 255:"It slowly resolved in my vision into a heap of mangled and bloodied white flesh in tattered Belgian para-commando uniforms. The men were piled on top of…"; A further standard work on the Rwandan genocide is the book: PHILIP GOUREVITCH, WE WISH TO INFORM YOU THAT TOMORROW WE WILL BE KILLED WITH OUR FAMILIES: STORIES FROM RWANDA (1998), at p. 150 "…Belgium withdrew from UNAMIR-precisely as Hutu Power had intended it to do. Belgian soldiers, aggrieved by the cowardice and the waste of their mission, shredded their UN berets on the tarmac of Kigali airport…The desertion of Rwanda was Hutu Power's greatest diplomatic victory to date and it can be credited almost single-handedly to the United States. With the Somalia debacle still very fresh, the White House had just finished drafting a document called Presidential Decision Directive 25…"; Sarah B. Sewall, *U.S. Policy and Practice Regarding Multilateral Peace Operations,* CARR CENTER FOR HUMAN RIGHTS POLICY WORKING PAPER 01-3, 2000, http://www.hks.harvard.edu/cchrp/Web%20Working%20Papers/PKO.pdf (last visited on Feb. 7, 2011): "…While PDD 25 as a policy still called for strengthening UN peacekeeping, the Administration encountered increasingly less political room to maneuver… Congressional antipathy toward peace operations congealed during the first year of the Clinton Administration. By late October 1993, Somalia had become the poster child for the failure of UN peacekeeping. Many Members, and particularly Republicans, feared that the Administration's peacekeeping policy was too proactive, overly supportive of the UN, and divorced from U.S. national interests…"

[38] *Fire Fight From Hell*, NEWSWEEK (Oct. 18, 1993), http://www.newsweek.com/1993/10/17/fire-fight-from-hell.html# (last visited on Feb. 6, 2011); George J. Church & Michael Duffy et al., *Somalia: Anatomy of a Disaster,* (Mon. Oct 18, 1993), http://www.time.com/time/magazine/article/0,9171,979399-9,00.html (last visited on Feb. 5, 2011): …" The later multinational operation was to have been the forerunner of a new kind of U.N. intervention, one mounted not to monitor a peace but to establish one, undertaken without the traditional invitation from a host government and carried out not by the usual lightly armed troops but by forces toting enough weapons to fight a serious battle.
But it now seems possible that Somalia will set a very different precedent -- of extreme U.S. reluctance to mount or join any peacekeeping operation except one that poses little or no risk of casualties…"; Evan Thomas, *Their Faith And Fears*, (Sept 9, 2002), http://www.newsweek.com/2002/09/08/their-faith-and-fears.html (last visited on Feb. 7, 2011): "…The Washington national-security establishment had become risk averse after the end of the cold war. Pace knew it firsthand: he had been deputy commander of U.S. troops in Somalia after the Battle of Mogadishu in 1993. "We were told to circle the wagons and not get Americans hurt…"

Casualty and war wariness contributes to the increased use of drones and radio controlled robots over the recent years.

Although ever expanding in their capabilities, such remote controlled devices are still mostly used for combat support roles – mainly reconnaissance and bomb defusing.[39] So far only the United States possesses a substantial number and various types of drones capable of being used in combat roles, which are increasingly used against suspected militants in Pakistan and Afghanistan.

As the steeply increased number of drone attacks in Pakistan and Afghanistan shows, it is only a question of time until there will also be unmanned vehicles operating on the ground and in part taking on the role of infantry men in fully fledged combat roles.[40]

It is conceivable that in the not too distant future such ground operating fighting vehicles (unmanned ground vehicles [UGVs]) can be air dropped together with a large number of low-priced sensors. This large number of small, economical sensors, operating as a network, could by infrared, thermal or audio-sensors used to locate enemy sniper positions and relay them to the ground operating fighting vehicles. Either radio operated by a soldier or autonomously operating[41], this technology could be used to engage snipers without putting any soldiers at risk.[42]

How to program such autonomous fighting vehicles is an entirely different, complex ethical issue. For example, what kind of ethics would need to be used: act utilitarian ethics or consequentialist utilitarian ethics? Concretely, such decisions would be used to determine what kind of ethical calculus an autonomously operating combat robot would use if it were to confront Osama Bin Laden surrounded by infant human shields. What would be the program's core value on how many innocent infant/civilian lives Osama Bin Laden was worth: 10? 20? 100? 1000? Would the calculus be different for slightly lower value targets such as Mullah Omar or Ayman Muhammad Rabaie al-Zawahiri? Could there be an "IF" condition used in the robot's computer code that would transfer control back to a human operator in situations of such difficult ethical constellations? If such a transfer to a human operator is feasible or practical under hectic battlefield conditions remains an entirely separate question. A "practicality" "IF" condition would be a further colossal coding challenge. While Isaac Asimov's famed three robotic laws[43] provide good guidance in the context of all conceivable civilian uses, it remains unclear how they could be adapted in a military context, as the "no harm to humans" principle would be difficult to uphold in a situation.[44] Possibly, the three robotic laws could be still upheld if autonomously operating combat robots were only allowed to target vehicles, buildings or caves (possibly even with humans inside), but would never be permitted to target humans in a "face-to-face" confrontation. The debate on Asimov's robotic laws, even in a military context, was revitalized, when a South African Army robot killed seven South African soldiers during a test exercise.[45]

The question of individual criminal responsibility under International Humanitarian Law (IHL) and law of armed conflict (LOAC) for acts committed by the autonomously operating robot is so far barely addressed by the scholarly literature. A leading thinker in the field, Ron Arkin of Georgia Tech, introduces the very helpful starting point of assigning responsibility to one operator for the mission of an autonomous robot.[46] The operator

[39] Cassandra A. Fortin, *Airman and his robot a bomb defusing team* (June 2, 2010), http://www.northwestmilitary.com/news/focus/2010/06/northwest-military-ranger-newspaper-mcchord-airlifter-airman-robot-bomb-defusing-team/ (last visited January 6, 2011); http://www.irobot.com/gi/ (last visited January 6, 2011); Erik Sofge, *Robotic Task Force: A Two-Robot, Bomb-Defusing, Riot-Controlling, Firefighting Team* (October 1, 2009 12:00 AM), http://www.popularmechanics.com/technology/engineering/robots/4313799 (last visited January 6, 2010).

[40] Pam Benson et al., *Intelligence, potential plot are factors in drone-attack increase- Administration's Evolving Counterterrorism Campaign Has Widened Assault with Greater Regional Cooperation* (September 28, 2010), http://articles.cnn.com/2010-09-28/world/pakistan.drone.intel_1_drone-missile-attacks-pakistan-taliban?_s=PM:WORLD (last visited January 6, 2011); *Obama Has Increased Drone Attacks* (Feb 12, 2010), http://www.cbsnews.com/stories/2010/02/12/politics/main6201484.shtml (last visited January 6, 2011); Dan Murphy, *Suicide attacks down, Predator drone exits, and other overlooked stories in 2010* (Dec 22, 2010), http://www.csmonitor.com/World/Global-Issues/2010/1222/Suicide-attacks-down-Predator-drone-exits-and-other-overlooked-stories-in-2010 (last visited January 6, 2010); Rasool Daward, *Record Level Of US Drone Attacks Hit Afghan Militants* (September 15, 2010, 12:59 AM), http://www.huffingtonpost.com/2010/09/15/record-level-of-us-drone-_n_717557.html (last visited January 6, 2011).

[41] P.W. Singer, Wired for War: The Robotics Revolution and Conflict in the 21st Century, 124-128 (2009)

[42] Apparently a robot currently being tested and called REDOWL (Robotic Enhanced Detection Outpost with Lasers) uses lasers and sound detection equipment to detect snipers…and instantly targets them with an infrared laser beam, see: P.W. Singer, Wired for War: The Robotics Revolution and Conflict in the 21st Century, 110 (2009)

[43] Apparently, these 3 laws were 1st introduced in Asimov's short story *Runaround* of 1942 and later elaborated in his *Robots* series (resulting in the popular movie *iRobot*). The content of these laws*:*

1.) A robot may not injure a human being or, through inaction, allow a human being to come to harm

2.) A robot must obey orders given it by human beings except where such orders would conflict with the First Law

3.) A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

[44] Some very good thoughts and basic sets of ethics instructions can be found in the work of Ron Arkin of Georgia Tech, such as: Ron Arkin, Governing Lethal Behavior in Autonomous Robots (2009) at p. 54 and 208.

[45] Priya Ganapati, *Robo-Ethicists Want to Revamp Asimov's 3 Laws*, WIRED, July 2, 2009, http://www.wired.com/gadgetlab/2009/07/robo-ethics/ (last visited Feb. 2, 2011).

[46] Ron Arkin, Governing Lethal Behavior in Autonomous Robots (2009) at p. 202.

would review and acknowledges the use of each obligation for the mission. The operator then confirms and types his name to accept responsibility for the conduct of the mission.[47] This is reminiscent of the command responsibility of officers for their soldiers and certainly addresses the issue of ethical conduct on operational level. However, the strategic level of the original programming/coding is not satisfactorily encompassed by this solution. The question of the individual criminal responsibility for the "collateral damage calculus" and computer code remains to be solved.

So far, developers and military planners are rather adamantly maintaining that ultimately humans will "stay in the loop."[48] However, the downing of Iran Air Flight 655 by a highly automated US destroyer's missile defense system or as the destruction of two allied planes during the second Gulf War by Patriot missiles show that already in many areas "the loop" of humans has been reduced to mere veto power. Therefore, the scenario of autonomous or at least "automatic" fighting robots might be closer than commonly assumed.[49]

Some military strategists assume that the speed, confusion and information overload of modern war will soon move outside of "human space."[50] The level of speed required on the battlefield certainly will increase beyond human capacity so that autonomously operating robots appear to be an inevitable development.[51] Some major military powers might have serious inhibitions regarding the use of such autonomous fighting systems. However the "prisoner dilemma" of "what if the other side gets it first" makes this inevitable development more likely. Thus, it is questionable if international treaty regimes banning such autonomous systems could be successful.

Before the large-scale introduction of autonomously operating robots becomes feasible, radio controlling robots will be the dominant means of operation.[52] The process of remotely controlling such robots will significantly differ from the button and joystick controlled present day approach. The progress made by brain controlled prosthetic limbs makes a scenario very probable where robots, capable of movement almost as precise as that of a human soldier, react to their controller's thoughts, which would provide such robots with previously unknown operational capabilities.[53]

In addition to the expanding combat roles of robots, their support roles will diversify and be capable of ever more complex operations such as Robotic evacuation vehicles which will be able to autonomously extract soldiers to safety and will enable human operators to conduct remote controlled surgeries inside the vehicle.[54]

Apart from conventional remote controlled robot, apparently recent *Defense Advanced Research Projects Agency* (DARPA) research has opened an alternative path, that of remote controlled animals such as in the so called "*robo*-rat" experiments.[55] In that experiment rodents were implanted electrodes in their brain through which the rats could be ordered to walk or climb through any path it was instructed to follow.[56]

As much as this would open up unknown capabilities to use such animals in mine-clearing or bomb detection operations, at the same time it raises considerable bioethics concerns regarding the morality

---

[47] Id.

[48] P.W. Singer, Wired for War: The Robotics Revolution and Conflict in the 21st Century, 124-128 (2009)

[49] Id.; Similarly, Israel's newest "Iron Dome" rocket defense system is capable of taking out even very small incoming rockets and artillery shells and apparently operates as an automated system. Especially given the small size of Israel and the speed of the incoming rockets the margins of the response time needed are minimal and might proof to overwhelm human operators, see: *Iron Dome system passes final tests*, THE JERUSALEM POST July 19, 2010 8:56 PM, http://www.jpost.com/Israel/Article.aspx?id=181936 (last visited Feb. 9, 2011).

[50] P.W. Singer, Wired for War: The Robotics Revolution and Conflict in the 21st Century, 124-128 (2009)

[51] Id.

[52] The possibility and feasibility of autonomously operating robots is mostly a question of the general progress of artificial intelligence (A.I.). Whilst in 1957 the AI crowd confidentially predicted that machines soon would be able to replicate all kinds of human mental achievements this turned out to be largely unachievable, in large part as the understanding of the human Brain is still limited. Most importantly, researchers noticed that they did not need to emulate human intelligence as a whole as intelligence revealed itself not to be a unitary thing but rather showed itself to be "all kinds of different" behaviors, see: Stephen Levy, *The A.I. Revolution*, WIRED, Jan. 2011, at 88; Thus, present day robotics follows this "insular" approach of certain kinds of intelligence(s). Often this type of AI is not even notice as such. Fittingly Google's cofounder Larry Page expressed that in 1978 typing queries into a machine and receiving access to all the world's knowledge would undoubtedly have been seen as a feat of AI[52]. The same applies to many present day personal robots who are able to "understand" and execute simple spoken commands, see: Stephen Levy, *The A.I. Revolution*, WIRED, Jan. 2011, at 88; interestingly by abandoning the old path of trying to emulate human intelligence we might be moving closer to true A.I. which in the foreseeable future might enable truly autonomously operating combat robots.

[53] JONATHAN MORENO, MIND WARS BRAIN RESEARCH AND NATIONAL DEFENSE, 39-40 (2006): In this book it is also described how a monkey succeeded controlling a robotic arm by a computer connected to his motor cortex. A group of Caltech scientists showed that intention can be read directly from activity in the parietal cortex.

[54] P.W. Singer, Wired for War: The Robotics Revolution and Conflict in the 21st Century, 112 (2009)

[55] Unbeknownst to the general public worldwide and to large parts of the American public DARPA quite possibly constitutes one of the most important research funding entities on planet. Given its influence DARPA is exceptionally lean with a budget of only 3 billion USD when compared to an overall 651 billion USD spending on defense activities in the United States in 2009. Countless research programs on US university campuses are funded by DARPA, quite often unknown to the (PhD) students benefitting from DARPA funding. Founded in the wake of the *Sputnik* shock, DARPA has influenced technological revolutions for beyond the military sector and is e.g. responsible for the development of the internet, GPS navigation, the Worldwide Standardized Seismograph Network (WWSSN), staggering advances in prosthetic limbs etc., see: Michael Belfiore, The Department of Mad Scientists- How DARPA is Remaking Our World From the Internet to Artifical Limbs (2009).

[56] Id. at 43.

of brain-controlling living creatures in such a way. This is especially worrisome and bioethics-relevant as this research might open up possibilities control human soldiers in the same way.[57]

However, the increased use of such remotely operated or even autonomous vehicles (or animals) not suitable to win any hearts and minds for external assistance forces such as the International Security Assistance Force for Afghanistan (ISAF) or local government forces. Even in the absence of combat robots, the counter insurgency scholar David Kilcullen criticized that heavily armored presence in civilian areas lead to a very de-humanized perception of coalition forces in Iraq. In his book, *The Accidental Guerilla*, he described this as follows: "We are aliens-imperial stormtroopers with our Darth Vader sunglasses and grotesque and cowardly body armor…the insurgents have done to us what we said we would do to them-isolated us from the population by using the IED, and…our penchant for technology and fear of casualties…"[58]

If already the present human presence is capable of creating such a de-humanized "alien" perception the chances of a truly robotic force of winning over hearts and minds appear to be very slim.

Additionally, the use of such unmanned ground or aerial vehicles certainly will result in saving the lives of numerous soldiers and helps the local security forces buy some time until their own capabilities have increased. At the same time, these techniques will risk more civilian lives in the countries of origin of these foreign security forces. If militants in conflict areas such as Afghanistan will no longer be able in a position to inflict substantial casualties to the foreign assistance forces, they might find it necessary to increase strikes on civilians in the home countries of these highly technologized foreign forces.[59]

The attacks of September 11, 2001, the Beslan school siege[60], the Moscow theater hostage taking[61] or the Mumbai shootings provide a good glimpse of how such strikes might look like.[62]

Nonetheless, one should bear in mind that drones and radio controlled combat robots will most certainly be used by insurgents as their prices further decrease and as companies such as iRobot[63] and Robotex[64] have started pioneering robots for consumer (and law enforcement) use. Most prolific terrorist/insurgent organizations for all their anti-modernist and anti-globalization missions have shown to be very apt in putting the tools of globalization quite aptly to their use (e.g. internet and cell phones). The use of robots will not form an exception to this.

4. Creating a new breed of *Über*-Soldiers

In addition to the possibilities of the increased "outsourcing" of combat to remote controlled fighting vehicles a further (admittedly a bit more distant) development which needs to be contemplated by defense strategists are the numerous possibilities for the enhancements of the individual soldiers themselves.

E*xternal* enhancements of soldiers such as through exoskeletons[65] need to be contemplated just as much as *internal* enhancements of soldiers such as by the deliberate use of prosthetic limbs (which in the not too distant future might not only be able to compete with natural limps but exceed their capabilities.[66] The first

---

[57] Id. At 44.

[58] David Kilcullen, The Accidental Guerilla: Fighting Small Wars in the Midst of a Big One (2009) at 136.

[59] P.W. Singer, Wired for War: The Robotics Revolution and Conflict in the 21st Century (2009), p. 313: "…the more we take American soldiers of the battle fields, the more we will drive them to hit home…".

[60] Peter Baker and Susan B. Glasser, *Russia School Siege Ends in Carnage Hundreds Die As Troops Battle Hostage Takers*, THE WASHINGTON POST (from Sept. 4, 2004) at p. A01, http://www.washingtonpost.com/wp-dyn/articles/A58381-2004Sep3.html (last visited Feb.7, 2011).

[61] *Moscow Gas Debacle Leaves Putin Unscathed*, TIME homepage (from Monday, Oct. 28, 2002), http://www.time.com/time/world/article/0,8599,385038,00.html (last visited Feb. 8, 2011); Nick Paton Walsh & Jonathan Steele, *Chechen gunmen storm Moscow theatre-Chechen gunmen hold 700 hostages after storming Moscow theatre* (from Thursday October 24, 2002 02.36 BST); http://www.guardian.co.uk/world/2002/oct/24/russia.chechnya (last visited on Feb. 8, 2011).

[62] *Gunfire heard at two Mumbai hotels*, CNN WORLD homepage (from Nov. 26, 2008), http://articles.cnn.com/2008-11-26/world/india.attacks_1_mumbai-hotels-cama-hospital-indian-police?_s=PM:WORLD (last visited Feb. 8, 2011); *What we know about the Mumbai attacks*, CNN WORLD homepage (from Nov. 27, 2008), http://articles.cnn.com/2008-11-27/world/mumbai.investigation_1_cafe-leopold-oberoi-three-gunmen?_s=PM:WORLD (last visited Feb. 8, 2011); *The Mayhem in Mumbai Making sense of India's terrorist attacks,* NEWSWEEK homepage (from Nov. 26, 2008), http://www.newsweek.com/2008/11/25/the-mayhem-in-mumbai.html (last visited Feb. 8, 2011).

[63] http://www.irobot.com/ (last visited on Feb. 10, 2011).

[64] http://www.robotex.us/micro.html (last visited Feb. 10, 2011), for their robot AvatarMicro Robotex even posts credentials of an Oakland SWAT team officer on their homepage.

[65] Duncan Graham-Rowe , *MIT Exoskeleton Bears the Load Researchers have developed a motorless exoskeleton that can carry 80 pounds,* MIT TECHNOLOGY REVIEW (from Sept. 26, 2007), http://www.technologyreview.com/Infotech/19433/ (last visited Feb. 8, 2008);
Andrew Valiente, Design of a Quasi Parallel Leg Exoskeleton to Augment Load Carrying for Walking (August 2005) (Thesis for a Master of Science at the MASSACHUSETTS INSTITUTE OF TECHNOLOGY Institute of Technology): "…Exoskeletons have application for military and service personnel, as well as for patients with muscular impairments. Exoskeletons have the ability to traverse non-paved terrain accessing locations where wheeled vehicles cannot. Exoskeletons promise to allow people to run farther, jump higher, and bear larger loads while expending less energy. Recent physiological studies suggest that it may be possible to build an orthotic exoskeleton to dramatically increase the locomotory endurance of service personnel. Simulated reduced gravity experiments have demonstrated that the metabolic cost of walking and running can be reduced by 33% and 75% respectively, if gravity is reduced by 75%..."

[66] See the case of CAS 2008/1408/Pistorius v. IAAF/award of 16 May 2008, where a disabled South African athlete, a double amputee since he was 11 months old, who ran on two prosthetic legs known as "*Cheeta Flex*" sued for his right to compete in the 2008 Olympic games. The International Association of Athletics Federations (IAAF) had original had

steps are already being undertaken to enable the user to brain-control such limps[67]) or artificial retinas.[68]

Such enhancement are not only restricted to *mechanical* or *implantation of technical devices based* enhancement but could also include biological alterations such as by controlling soldiers' energy metabolism on demand (e.g. by inducing some kind of hibernation stage to seriously wounded soldiers).[69]

The legal and ethical implication for such developments are tremendous and have so far not sufficiently been reflected in the scholarly literature[70] and it remains uncertain how societies would react to a military caste or *de facto* species of soldier with genuinely distinguishable physical features (not dissimilar to soldier ants in many ant societies). The creation of such a *species/breed* of soldier would also raise challenges to democracy as such. The main challenge is twofold: How would such a caste of *Über*-soldiers see themselves and their loyalty to a democratic leadership and how careful or careless would the broader public vote on combat deployment of such a distinguishable species? Would the public be less concerned about a high rate of losses of such a distinguishable case?

The current situation of a widening "civil-military gap"[71] and the tendency that the military in most developed (especially Western nations) is increasingly being concentrated in *Mega*-bases[72] in thinly populated provincial areas (and thereby disappear out of society's sight) strongly suggests that with a distinguishable military species society would be significantly less concerned about the lot of their military caste.

The answers of societies to the "if" and "how" of such a new soldier species very much depend on the level of threat a society is faced with.[73] A society under an existential threat most likely will take a different position to such a soldier caste or species than a peacetime society not facing such existential threats.

However, such enhancement possibilities certainly are closer and less "science fiction"-like than they do

---

rejected his request and appeal based on IAAF Rule 144.2(e) states that "For the purposes of this Rule, the following shall be considered assistance, and are therefore not allowed: […] (e) Use of any technical device that incorporates springs, wheels, or any other element that provides the user with an advantage over another athlete not using such a device". The mere fact that it was even considered that this technical device would provide him with an advantage over able bodied athletes on the highest professional level clearly shows the tremendous progress made in the technology of such prosthetic limbs and that it might be probable that such prosthetic limbs might soon exceed natural limbs in their capacities.

[67] Henry T. Greely, *Law & the Revolution of the Neuroscience: An early look at the field,* Akron Law Review, 2009, at 698.

[68] Department of Ophthalmology School of Medicine and Hansen Experimental Physics Laboratory, Stanford University *Restoration of Sight to the Blind: Optoelectronic Retinal Prosthesis* http://www.stanford.edu/~palanker/lab/retinalpros.html# (last visited January 6, 2011).

[69] Jonathan Moreno, Mind Wars Brain Research and National Defense, 122 (2006)

[70] One of the laudable exceptions is Jonathan Moreno's Book: Id.

[71] Thomas E. Ricks, *The widening gap between the military and society: U.S. military personnel of all ranks are feeling increasingly alienated from their own country, and are becoming both more conservative and more politically active than ever before. Do they see America clearly?* THE ATLANTIC MONTHLY ELECTRONIC EDITION (from July 1997), http://www.theatlantic.com/past/docs/issues/97jul/milisoc.htm (last visited on Feb. 8, 2011); Thomas S. Szayna, Kevin F. McCarthy et al., *The Civil-Military Gap in the United States Does It Exist, Why, and Does It Matter?* Prepared for the US Army by RAND Arroyo Center (2007).

[72] Tadlock Cowan & Oscar R. Gonzales, *Military Base Closures: Socioeconomic Impacts,* CRS Report for Congress (Jan. 25, 2010); http://www.fas.org/sgp/crs/natsec/RS22147.pdf (last visited on Feb. 8, 2011); *Base Realignment and Closure (BRAC)*, http://www.globalsecurity.org/military/facility/brac.htm (last visited on Feb.8, 2011); Karen Jowers, AirForceTimes (from Monday Feb 7, 2011 15:50:14 EST), http://www.airforcetimes.com/news/2011/02/military-brac-bases-traffic-020711w/ (last visited on Feb. 8, 2011); *Bryan Bender*, Military cuts are sharpest in New England Officials worry for security, culture*, The Boston Globe April 10, 2005, http://www.globalsecurity.org/org/news/2005/050410-military-cuts.htm (last visited on Feb. 8, 2011): "New England has experienced a greater decline in military presence since the end of the Cold War than any other region of the country and is now at risk of losing its only active-duty air and naval bases, according to data compiled by the Globe and government officials. Thirty-five of 93 major bases shuttered across the nation since 1988, or a third of the total, were in Northeastern and Midwestern states, part of an exodus of large military installations from Northern states over the last decade and a half to the economically friendlier South and West. The six New England states saw the largest drop in active-duty personnel over the period. Nearly 60 percent of full-time military personnel based in the region went away as their installations were closed by decisions of four Base Realignment and Closure commissions, the last in 1995. In 1988, New England was home base for 30,600 active-duty personnel. It is currently home to less than 12,700. Now, New England is bracing to save the operational units that are left: its only remaining air base, in Brunswick, Maine, and only naval base, in New London, Conn… ''What concerns me is how the forces are moving to a red state-blue state bifurcation," said John Pike, a military scholar at GlobalSecurity.org in Alexandria, Va. ''Most of the bases are in the red states, and the bases in the blue states are mainly in red congressional districts. The military is a normal part of society in red states and not a normal part of society in many blue states…" "In Massachusetts alone, the number of military personnel dropped by 74 percent between 1988 and 2002, from 9,335 to 2,427, far higher than the 24 percent reduction nationwide, according to government statistics compiled by the Northeast-Midwest Institute, a military lobbying group. Maine had a 54 percent drop, from 5,849 to 2,689, according to the institute. The reduction was even more precipitous in New Hampshire, where the number of active-duty personnel in the state went from 4,143 to 326, a 92 percent drop and the largest slide in the nation. It was part of a wider trend. Across the entire Northeast the drop in military personnel was 37.5 percent. In the Midwest it was 46.6 percent. But the West only saw a 30 percent drop, while the South witnessed a mere 15 percent slide. ''There is an unmistakable societal consequence if we create a military without ties, in the form of active duty bases, in every part of the country," said Senator John F. Kerry, Democrat of Massachusetts…"*

[73] It remains a valid question where to draw a distinction between "artificial" enhancements and "natural" enhancements such as exercise, see also: JONATHAN MORENO, MIND WARS BRAIN RESEARCH AND NATIONAL DEFENSE, 133 (2006).

appear and therefore need to be addressed by the leading military scholars *before* they become reality.

5. The International Humanitarian Law (IHL) and Law of Armed Conflict (LOAC) implications of *cyber warfare* and anti-satellite warfare-Collateral damage beyond mere virtual damage & the new "mutual assured destruction" of the cyber-age:

Interestingly, some scholars who are deeply immersed in the topic of *cyber-attacks* or even *cyber warfare* appear to underestimate both the reality of cyber-warfare and its potential civilian collateral damages.

In a blog[74] published by the University of California in Berkeley, Stephen Maurer disputed a well-known computer scientist's complaint that cyber war was the "real WMD" and that America needed to spend less money on nuclear weapons defense.[75] Maurer attributed this WMD statement rather cursory to the fact that "people who spend weeks on end filling out grant applications are apt to say silly things."[76] Moreover, Maurer added that he had never heard anyone claim that Cyber War can inflict casualties on a nuclear scale. Additionally, the author raised the crucial question if cyber war qualified "as War on any scale at all."[77]

To Maurer problems only become "Wars" "when you run out of reasonable alternatives to calling in the military."[78]

Maurer disputed the validity of headlines of the Russia-Georgia conflict of 2008 such as "Cyber War is Official."[79] To Maurer instead of a cyber-war this conflict rather saw a number of "patriotic hackers" (= civilian amateurs or mobilized criminals) committing the same Cyber Crimes that the world's IT managers see on a daily basis.[80]

Maurer stressed that Microsoft received millions of error reports from users every day. However, he pointed out that in this case the number of eyeballs currently looking for vulnerabilities was incomparably larger than the world's population of Cyber Criminals and Cyber Vandals so that even State-funded searches became "a drop in the ocean."[81]

Maurer ended his reflection with the conclusion that certainly there was good reason that Defense Department should fund Cyber Crime research to protect its own systems and everyone else's. However, Maurer pointed out that this was already occurring in the *old* "cyber crime" context. To Maurer "cyber war" rhetoric constituted an unnecessary escalation – and an expensive one at that.[82]

Maurer's reflections were included in this paper, as he managed to muster a wide array of conceivable counter arguments to the reality of cyber warfare.[83] The limited concern assigned to cyber warfare in Maurer's blog reflected how to a large part of the general public cyber warfare still appears to have only virtual, i.e. cyber space ramifications,[84] seemingly without "real" work effects and damages.

This public underestimation of cyber warfare is bound to change after the highly effective "Stuxnet" computer virus attack on Iranian industrial and factory systems and which apparently targeted Busher nuclear

---

[74] "The Berkeley Blog-Topical Questions, Campus Experts and Public Opinion from UC Berkeley".

[75] Stephen Maurer, *Keeping the Cyber-Peace*, The Berkeley Blog, Topical Questions, Campus Experts and Public Opinion from UC Berkeley (Feb. 19, 2010), http://blogs.berkeley.edu/category/science/20091111/?full=1 (last visited Jan. 6, 2010).

[76] Id.

[77] Id.

[78] Id.

[79] Id. Maurer attributes this headline to *Aviation Week* in its edition from Sept. 14 2009.

[80] Id.

[81] Id.

[82] Id; Admittedly, Maurer's considerations have been assigned a rather large portion in this paper, especially given that he is not a leading scholar and as his position at the time of the drafting (in the last quarter of 2009) was a minority view in the scholarly literature and the public debate: Especially given that before the publication of Maurer's blog major military powers had publically admitted to take the threat of cyber war very seriously: Doug Tygar, *UCB leader in critical infrastructure protection research*, The Berkeley Blog, Topical Questions, Campus Experts and Public Opinion from UC Berkeley (Nov. 9, 2009), http://blogs.berkeley.edu/category/science/20091111/?full=1 (last visited Jan. 6, 2011): …Cyberwarfare is something that is taken seriously by the Chinese and Russian military. Officers in the (Chinese) People's Liberation Army have written treatises on cyberwarfare. And we have extensive evidence of successful penetrations of US governmental and military sites. The US also takes cyberwarfare seriously: Defense Secretary Gates announced on June 23rd a new "US Cyber Command" (part of the US Strategic Command). While protection of government and military computer systems is a priority of the first order, the US is even more vulnerable to electronic attacks on the civilian critical infrastructure. These attacks are not merely a hypothetical possibility, as President Obama discussed in his May 29 remarks…; Tim Reid, *China's cyber army is preparing to march on America, says Pentagon,* The Times-The Sunday Times (Sept. 8, 2007), http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2409865.ece (last visited Jan. 6, 2011); Spencer Ackerman, *It Begins: Military's Cyberwar Command Is Fully Operational*, (from Nov.4 2010), http://www.wired.com/dangerroom/2010/11/it-begins-militarys-cyberwar-command-is-fully-operational/ , last visited on Feb. 5 2010); The concern of major military powers with cyber warfare was strengthened, well before Maurer's blog, after the after severe cyber-attacks e.g. on Google, Intel, Adobe, the Dalai Lama's government in exile: Doug Tygar, *Cyberwar,* The Berkeley Blog, Topical Questions, Campus Experts and Public Opinion from UC Berkeley (Feb. 23, 2010), http://blogs.berkeley.edu/category/science/20091111/?full=1 (last visited Jan. 6, 2011)

[83] Interestingly even high ranking "cyber war" officials downplay the existence of something worthy the name cyber war: Ryan Singel, *White House Cyber Czar: 'There Is No Cyberwar'*, (from March 4, 2010), http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/ , (last visited on Feb. 5, 2011).

[84] Monish Shah, *Shah: Prepare for cyber-warfare* (Nov. 12, 2010), http://www.yaledailynews.com/news/2010/nov/12/shah-prepare-cyber-warfare/ (last visited Jan. 6, 2011)

power plant has been described as one of the "most refined pieces of malware ever discovered."[85]

Experts described that the malicious software, first detected in June last year, was almost certainly designed to make damaging, surreptitious adjustments to the centrifuges used at Natanz, Iran's uranium enrichment site.[86] Separate investigations by US nuclear experts have discovered that "Stuxnet" worked by increasing the speed of uranium centrifuges to breaking point for short periods. At the same time it shut off safety monitoring systems, hoodwinking operators that all was normal.[87]

"Stuxnet" illustrates what has been largely neglected in both Law of Armed Conflict (LOAC) and International Humanitarian Law (IHL) both in the scholarly discussions and the curricula of military academies.[88] LOAC and IHL attempt to limit unnecessary suffering during armed conflicts. IHL is especially relevant for cyber warfare as IHL tries to protect the civilian population and to limit the damage to civilian infrastructure.

The "Stuxnet" cyber-attack demonstrates that the imperatives for proportionality in causing civilian harm are comparable to e.g. the bombardment of a bridge which has dual civilian and military use. In case of an attack on such a *dual use* target, it needs to be determined first if the target has a sufficiently important military use in order to justify an attack as such. Additionally, once it is determined that indeed the military use is sufficient to launch an attack, it needs to be determined what would be the number of expected civilian casualties and the expected damage to the civilian infrastructure. Once it is concluded that the reasonably expected civilian casualties and infrastructure damages are not disproportionate to the expected military gains in destroying the target, every precaution must be taken to minimize the probability of civilian casualties and destruction of civilian infrastructure.

Likewise in the case of cyber-attacks such as the "Stuxnet" operations the collateral damages of such a virtual attack need to be minimized. Even if the attack is "only" virtual, indiscriminate attacks can cause disproportionate civilian casualties and immeasurable damage to civilian infrastructure.

In the case of "Stuxnet" it is very probable that the "Stuxnet" virus constitutes an indiscriminate attack as it is not only capable of harming the suspected target, the Busher nuclear power plant's centrifuges, but also any industrial and factory systems. It is conceivable that this virus could also attack factories producing crucial medicines or life saving devices. The number of potentially resulting civilian casualties could theoretically be just as high as in the case of e.g. carpet bombing a bridge with dual civil military use.

The existing literature supports this view and stresses that even in the case of "only" virtual, i.e. cyber-attacks the known principles of *distinction*, as stipulated in Art. 48 Additional Protocol to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) clearly states the imperative distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives. Additionally (Art. 51 AP I) stipulates that indiscriminate attacks are prohibited.

Indiscriminate attacks are:

"(a) those which are not directed at a specific military objective;
(b) those which employ a method or means of combat which cannot be directed at a specific military objective; or
(c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol;
and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction."[89]

Apart from the indiscriminate nature and the high likelihood of civilian collateral damage (even if "only" in the form of exorbitant financial costs to the civilian population, whilst actual loss of life and limb certainly is not an unlikely result in such cyber-attacks) through such cyber-attacks the problem of proliferation arises. In the past the mere term and the legal regimes connected to

[85] Josh Halliday, *Stuxnet worm is the 'work of a national government agency' Malware believed to be targeting Iran's Bushehr nuclear power plant may have been created by Israeli hackers*, The Guardian (Sept. 24, 2010), http://www.guardian.co.uk/technology/2010/sep/24/stuxnet-worm-national-agency (last visited Jan. 6, 2011); *A cyber-missile aimed at Iran?* The Economist (Sept. 24, 2010), http://www.economist.com/blogs/babbage/2010/09/stuxnet_worm (last visited Jan. 6, 2010).

[86] Christopher Williams*, Stuxnet: Cyber attack on Iran 'was carried out by Western powers and Israel' A British security expert has uncovered new evidence in the Stuxnet virus attack on Iran's nuclear program*, THE TELEGRAPH, Jan. 21, 2011, http://www.telegraph.co.uk/technology/8274009/Stuxnet-Cyber-attack-on-Iran-was-carried-out-by-Western-powers-and-Israel.html (last visited Feb. 8, 2011).

[87] Id.

[88] Which does not mean that there are no articles on this subject. To the contrary, there are a number of good recent articles on this subject, however, compared to the publication density of other areas of LOAC or IHL they are still comparably scarce: Eric Talbot Jenssen, *Cyber Warfare and Precautions Against the Effects of Attacks*, TEXAS LAW REVIEW, Jun 2010, 1522-1556L; Knut Dörmann, *Computer network attack and international humanitarian law*, *Extract from The Cambridge Review of International Affairs "Internet and State Security Forum"* (19 May 2001), http://www.icrc.org/eng/resources/documents/misc/5p2alj.htm (last visited Jan 6, 2010); Jeffrey T.G. Kelsey, *Hacking into International Humanitarian Law*, *The Principles of Distinction in the Age of Cyber Warfare*, MICHIGAN LAW REVIEW Vol. 106, 1427, 1450 (2008); Dr. Rex Hughes, *Towards a Global Regime for Cyber Warfare*, Chatham House, London (2009).

[89] See also: Knut Dörmann, *Computer network attack and international humanitarian law*, *Extract from The Cambridge Review of International Affairs "Internet and State Security Forum"* (19 May 2001), http://www.icrc.org/eng/resources/documents/misc/5p2alj.htm (last visited Jan 6, 2010).

"proliferation" seemed to be reserved to Weapon of Mass Destruction (WMD). With the advent of powerful cyber-attack programs such as "Stuxnet", the uncontrolled proliferation of such programs (whether in the form of worms, viruses or any other malware) the problem of "proliferation" also extents to these virtual "WMDs."[90]

"Stuxnet" spread far beyond its intended target to countries as distant as China and Germany, Kazakhstan and Indonesia.[91] This could support argument of the "Stuxnet" operation having been an indiscriminate attack which should be subjected to the same principles and prosecution as non-virtual attacks in IHL.

The same considerations for the IHL implications for cyber warfare clearly can be applied to satellite warfare as the consequences would be just as indiscriminate and potentially disastrous, especially as most satellites share the dual use characteristics of most cyber networks. The consequences of communication or navigation satellites being targeted and disabled[92] would be just as disastrous, as they could result in super tankers or planes crashing or colliding due to hampered navigation.

One mildly comforting fact remains for both cyber and satellite warfare. It appears to be immensely difficult to limit the effects and to provide effective protection against enemy attacks which poses the very real risk of mutual assured destruction.[93]

Most modern armies and societies are so dependent on the functioning of their information technology (IT) and their satellite technology, that any *cyber attack* and the following retaliation has the potential to be catastrophic on every fiber of the military machinery and society as a whole. It can therefore be presumed that all rational state actors are aware of such a very real possibility of mutual assured destruction and would be very much interested in limiting this tool of warfare. If the same would be true for isolated, totalitarian "rogue" states or desperate societies facing defeat remains to be seen.

While most major militaries even appear to have developed (highly classified) Rules of Engagement (ROE) for the use of cyber tools as a means of warfare, so far no overt or prominent "first strike"[94] vs. retaliation doctrine has emerged.

6. What does constitute an "armed attack" in *cyber*-space?

Directly related to these doctrinal issues and the topic "mutual assured destruction", it remains neglected *what* actually does constitute an all-out *cyber-attack*/use of force in cyberspace and *what* sets it apart from the scale and scope of a "normal" *cyber* vandalism. Concerning the wealth of doctrinal works surrounding the definitions of armed attack under Art. 51 Chpt. 7 of the UN Charter, works analogizing these doctrines to *cyber-attacks* are very scarce.

The Estonian and Georgian *cyber-attacks* from 2007 and 2008 have been a first test case further develop theories about *cyber-warfare* with the key questions being how to define it, whether to engage in it, and how to defend against it.[95] Some commentators argue that for a *cyber-attack* to qualify as "*cyber-war*" it would need to take place alongside actual military operations.[96] This can be analogized to the earliest operations against communications infrastructure. For instance during the American Civil War, a landing party from a Union navy steamer, went ashore to cut the telegraph lines between Fredericksburg and Richmond.[97] The Russian navy pioneered the use of radio jamming in the Russo-Japanese war of 1905. *Cyber-attacks* on infrastructure would constitute a further logical step in this tech warfare evolution.[98] The attacks on Georgia might qualify as *cyber-warfare* by this definition, but those on Estonia would not, since there was no accompanying military offensive in the real world.[99] Some commentators phrase this concept rather concisely as "For it to be *cyber-war*, it must first be war in first place."[100]

Many scholars do not concur with this condition. A "digital Pearl Harbor" is conceivable as an unexpected

---

[90] Gregg Keizer, *Why did the Stuxnet Worm spread? Propagation hints that first attack failed, say researchers* (October 1, 2010 01:02 PM)

[91] Id.

[92] Sharon Weinberger, *Return of the Killer Satellite Weapons* (April 23, 2007), http://www.wired.com/dangerroom/2007/04/return_of_the_k/ (last visited January 6, 2010).

[93] Reminiscent of KARLS JASPERS, THE ATOM BOMB AND THE FUTURE OF MANKIND, 1961; see also: http://plato.stanford.edu/entries/jaspers/ (last visited January 6, 2011); Colonel Charles Williamson, of the intelligence and surveillance division of America's air force, proposed that the United States should establish its own "botnet"—a network of machines "that can direct such massive amounts of traffic to target computers that they can no longer communicate and become no more useful to our adversaries than hunks of metal and plastic." America, he wrote, "needs the ability to carpet-bomb in cyberspace to create the deterrent we lack." The botnet could be built out of obsolete computers that would otherwise be discarded, he suggested. Such as botnet would be an excellent tool to retaliate again an earlier all-out cyber attack, see: *Marching off to cyberwar he internet: Attacks launched over the internet on Estonia and Georgia highlight the difficulty of defining and dealing with "cyberwar",* THE ECONOMIST, Dec 4, 2008, http://www.economist.com/node/12673385?story_id=12673385 (last visited on Feb. 10, 2011).

[94] John King, *Bush outlines first-strike doctrine*, http://articles.cnn.com/2002-09-20/politics/bush.national.security_1_military-force-policy-attacks?_s=PM:ALLPOLITICS (last visited on Feb. 4, 2011); Ian Traynor, *Pre-emptive nuclear strike a key option, NATO told*, The Guardian, Jan. 22, 2008, http://www.guardian.co.uk/world/2008/jan/22/nato.nuclear (last visited on Feb. 5, 2011).

[95] *Marching off to cyberwar-The internet: Attacks launched over the internet on Estonia and Georgia highlight the difficulty of defining and dealing with "cyberwar",* THE ECONOMIST, Dec 4, 2008, http://www.economist.com/node/12673385?story_id=12673385 (last visited Feb. 10, 2011);

[96] Id.

[97] Id.

[98] Id.

[99] Id.

[100] Id.

attack on a nation's infrastructure via the internet, in which power plants are shut down, air-traffic control is sabotaged and telecoms networks are disabled.[101] This would not necessarily need to be accompanied by conventional warfare. As the *cyber-attack* alone could paralyze the targeted society (especially if the targeted society has a more powerful conventional military) there would be no need to reinforce it with conventional force.[102]

The strongest definition of *cyber-war* requires that *cyber attacks* cause widespread harm, rather than mere inconvenience. The Georgian attacks did not cause physical harm, unlike the military operations going on at the same time.[103]

All sorts of "translation problems" arise when trying to apply existing international rules relating to terrorism and warfare to online attacks.[104] The United Nations Charter prohibits the use of force except in self-defense or when authorized by the Security Council. However, as explained there is little doctrinal framework on what counts as "the use of force" in *cyberspace.*[105] Clarity is needed with concerns to the minimal threshold that needs to be crossed in order to constitute an *attack*. It can be debated if a Denial of Service (DoS) attack would cross that threshold.[106] Not only the *type* of attack needs to be contemplated but also *what* would be targeted: would an attack on the media sector suffice or would rather be an air controlling facility the target of the attack?[107] An interesting idea in this debated is the requirement that effects to be produced by a *cyber-attack* would constitute an armed attack if the same effects could only be produced by an all out conventional military attack.[108]

In the sense of Article 51 of the U.N. Charter, it is likely that the *cyber-attack* would be treated as an armed attack. Similarly, if a *cyber-attack* had the same effects and was otherwise similar to government-initiated coercive or harmful actions that are traditionally not treated as the "use of force,"[109] such a *cyber-attack* would likely not be regarded as an action justifying a use of force in response.[110] Such a "similar effect" (compared to a conventional attack) doctrine constitutes a helpful starting point in creating a new conceptional framework. However, this concept has its limits as it does not differentiate among the innate levels of danger of different targets effected (the previous example of media vs. air control facilities). Also, it makes it systematically difficult to separate the potential effects of a comparable conventional attack from the effects of other means short of armed attack. For instance, an argument could be made that the failure of a (coal burning) power plant due to a *cyber-attack* could have only been caused by a comparable conventional bomb raid on that power plant. However it is also imaginable that the same power cut could have been caused by a coal embargo which would have the same effect.

Reaching consensus on the threshold of an attack is crucial especially in the context of military alliances such as NATO where the member states are treaty-bound to respond to an attack on any of their members and might be able to turn a limited regional conflict into a substantially larger crisis.[111]

7. The *Black Swans* of defense policy-common statistical fallacies in the prediction of future threats to security:

As described under the first paragraph of this article, there appears to be overwhelming consensus that the future of military involvement belongs to operations in counterterrorism and counterinsurgency.

Without venturing into *Popperian*[112], *Kuhnian*[113] or Lacatosian[114] *meta*-theoretical considerations on the development of such widely shared theoretical assumptions the underlying paragraph reflects on their origins, their innate danger and why they are symptomatic for modern societies.

In this day and age widely shared assumptions and predictions of the celebrated "analysts" of all fields are firstly derived by the interpretation of vast amounts of data of past events. The obsession of modern day societies with gathering information and intelligence[115] leads to an immense number of data which is then extrapolated to make predictions on future events (or at least their likelihood).

The influence of the devoutness to these complex probabilistic systems[116] can be seen in every aspect of

[101] Id.
[102] Id.
[103] Id.
[104] Id.
[105] Id.
[106] Id.
[107] Id.
[108] Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, JOURNAL OF NATIONAL SECURITY LAW & POLICY [Vol. 4:63, 2010], p. 73, http://www.jnslp.com/read/vol4no1/06_Lin.pdf (last visited Feb. 10, 2011).
[109] Such as: economic sanctions, espionage, or covert actions such as planting information or influencing elections, see: Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, JOURNAL OF NATIONAL SECURITY LAW & POLICY [Vol. 4:63, 2010], p. 73, http://www.jnslp.com/read/vol4no1/06_Lin.pdf (last visited Feb. 10, 2011).
[110] Id.
[111] Id.
[112] Karl Popper, The Logic of Scientific Discovery (1934); Karl Popper, Conjectures and Refutations: The Growth of Scientific Knowledge (1963).
[113] Thomas S. Kuhn, The Structure of Scientific Revolutions (1962).
[114] Lacatos argued that one research programme (i.e. a theory) can be described as progressive while its rivals are degenerating. A progressive research programme is marked by its growth, along with the discovery of stunning novel facts, development of new experimental techniques, more precise predictions, etc. A degenerating research program is marked by lack of growth, or growth of the protective belt that does not lead to novel facts: published in John Worrall & Gregory Currie (eds.) The Methodology of Scientific Research Programmes: Volume 1: Philosophical Papers (Philosophical Papers Vol. I), (1980).
[115] Drury D. Stevenson, *The Effect of National Security on the Criminal Law Paradigm*, Working Paper Series (September 1, 2010), http://ssrn.com/abstract=1669832 (last visited Feb. 8, 2011), at p. 3.
[116] Which at times appear to amount to little more than esoteric numerology.

modern societies, most notably in the financial markets, the insurance sector, criminal law policy (and the correctional system)[117] and defense policy.

Particularly highly developed societies show a strong obsession of avoiding uncertainty and trying to achieve the utmost risk minimization through their highly developed insurance sectors.[118] This basic tendency can be observed in all the aforementioned sectors and is fundamentally (re-) shaping them.

This reshaping is very prominent in the sector of criminal law. It is observed in scholarly literature that currently we are witnessing a shift toward focusing on incapacitation and prevention of crime rather than traditional deterrence or retribution.[119] Whereas the emphasis of criminal law in previous eras was punishing the blameworthy (retribution) or saving people from themselves (deterrence), the new focus is on preserving a comfortable, secure way of life, and law is approached as a method of eliminating risks.[120] When elements of deterrence are incorporated, the new paradigm shifts the focus toward lowering the rewards of illegal activity (by foiling terrorist plots or conspiracies before they succeed)[121] or raising the transaction costs[122] for criminals rather than traditional deterrence, which focused on the threat of punishment.[123]

Accordingly, in criminal law policy funding is allocated towards these large data analysis and to the incapacitation/prevention efforts found most efficient to maintain society's uncertainties and preserve a "secure" way of life.[124]

In the financial sector such number analysis and limitation of uncertainty has taken a dynamic of its own. Based on the analysis of vast amounts of data nowadays the complex models are being used by sophisticated programs and computers. These computers and programs are not limited anymore to "number crunching" but make actual decisions.[125] By some estimates computer aided high frequency trading now accounts for about 70% of total trade volume.[126]

What does this mean for defense policy, the interpretations and the predictions by the "analysts" and scholars? Most crucially, it can be noted that analysts and scholars cannot escape the background of the data and data-analysis obsessed societies that they are part of.

Therefore, it is hardly surprising that they apply the same tools and derive their predictions in the same fashion that for instance economists use in order to predict future developments in the markets.

The strength of developed societies and the whole data analysis culture lies in the substantial proficiency in managing the known risks.

However the *Achilles Heel* of such a model/culture lies in the unknown dangers, the *Black Swans*[127] of what can be expected based on experience and empirical knowledge.

Black Swan logic makes what you do not know far more relevant than what you do know.[128] One example is the terrorist attacks of September 11, 2001. Had the risk of a non-state actor launching an air attack of that magnitude been deemed *conceivable* and thus worthy of preventive action, the event would not have happened.[129] An additional example is the German invasion of France 1940. Based on their experiences with the German advances through Alsace-Lothringen in 1870 or Flanders in 1914 the French had built the famed fortified *Maginot* Line to prevent the same routes of attacks. The *Maginot* Line had one decisive gap at along the Ardennes as it was found inconceivable that any larger army, let alone a modern heavily mechanized army could advance through this hilly, forested area with its narrow roads. Yet that was exactly what the German army did.[130] Early reports by French reconnaissance airplanes on gigantic (and very vulnerable) German troop concentrations in the Ardennes were largely ignored.[131] The *Black Swan* of the "*inconceivable"* modus operandi of the German army led to the defeat of the

---

[117] Drury D. Stevenson, *The Effect of National Security on the Criminal Law Paradigm*, Working Paper Series (September 1, 2010), http://ssrn.com/abstract=1669832 (last visited Feb. 8, 2011).

[118] This observation was expressed by Prof. Drury D. Stevenson during the presentation of hiss paper *The Effect of National Security on the Criminal Law Paradigm* during the DEFENSE POLICY SYMPOSIUM on Jan. 22, 2011 at Stanford Law School.

[119] Drury D. Stevenson, *The Effect of National Security on the Criminal Law Paradigm*, Working Paper Series (September 1, 2010), http://ssrn.com/abstract=1669832 (last visited Feb. 8, 2011), p.9.

[120] Id.

[121] Id.

[122] Id. at p. 12; Airport checks are as well such instruments of incapacitation which considerably raise the transaction costs of would be terrorists.

[123] Id. at p. 9.

[124] Id. at p. 4.

[125] Felix Salmon & Jon Stokes, *Bull vs. Bear vs. Bot,* WIRED Jan. 2011, p.91.

[126] Id.; this prevalence of computer trading and automated decision making prompted the "Thinking machines" entrepreneur and MIT graduate William D. Hillis to the statement: "The computers are in control, we just live in their world".

[127] The "Black Swan" is a popular concept to illustrate the concept and problem of induction in logic courses in philosophy and mathematics. Until about the middle of the previous century induction was treated as a quite specific method of inference: inference of a universal affirmative proposition (All swans are white) from its instances (*a:* is a white swan, *b:* is a white swan, etc.) The method had also a probabilistic form, in which the conclusion stated a probabilistic connection between the properties in question. It is no longer possible to think of induction in such a restricted way; much synthetic or contingent inference is now taken to be inductive; some authorities go so far as to count all contingent inference as inductive, see: *The Problem of Induction*, STANFORD ENCYCLOPEDIA OF PHILOSPHY, *First published Wed Nov 15, 2006; substantive revision Mon Jun 21, 2010*, http://plato.stanford.edu/entries/induction-problem/ (last visited Feb. 9, 2011).

[128] Nassim Nicholas Taleb, THE BLACK SWAN: THE IMPACT OF THE HIGHLY IMPROBABLE (2007).

[129] Id., p. xxiii.

[130] Dr. Gary Sheffield, *The Fall of France,* BBC homepage series World Wars in-depth, last updated Aug. 9, 2010, http://www.bbc.co.uk/history/worldwars/wwtwo/fall_france_01.shtml (last visited Feb. 9, 2011).

[131] Julian Jackson, THE FALL OF FRANCE: The Nazi Invasion of 1940 (2003), p.42.

French army and the British expeditionary corps in just 6 weeks.[132]

The philosopher and statistician Nassim Nicholas Taleb in his bestselling book "THE BLACK SWAN: THE IMPACT OF HIGHLY IMPROBABLE" describes the pattern of "clustering" according to which journalists tended to cluster not necessary around the same opinions but frequently around the same framework of analyses.[133] According to Taleb they assigned the same relevance to the same sets of circumstances and divided their observations into the same categories.[134]

It is not improbable that such clustering is responsible for the widely shared believes of scholars and practitioners that for the foreseeable future counterinsurgency or counterterrorism are the only games in town. Every other "inconceivable" type or intensity of warfare has the possibility of being the next "Black Swan".

Referring to Bertrand Russel, Taleb describes the prolific philosophical question of how one could logically go from specific instances to reach general conclusions.[135] This is commonly referred to as the Problem of Induction or the Problem of Inductive Knowledge.[136] To illustrate this problem Taleb uses the turkey[137] analogy from Bertrand Russel according to which the turkey learned, based on its observation, it will receive an increased number of friendly feedings with every new day. As this has been its experience from the past 1000 days it is reasonable to assume that this will provide sufficient data to predict future developments.[138] However, on the 1000th day the unexpected happens to the turkey. It is remarkable that in this example the risk was the highest when the turkey's confidence was at its highest level as well.[139] This can be analogized to the nature of any prediction of future events based on the experiences with past events, albeit within the limitations of every analogy in relation to the reality it refers to.[140]

Nonetheless, with the intrinsic limitations of any analogy it is worth posing the hypothetical question who would be the turkey and who would be the butcher if the analogy were to be applied. Certainly the "surprise" will be on the turkey's and not the butcher's side.[141]

As a further example Taleb refers to the summer of 1982 when large American banks had almost their entire earnings wiped out. They had been lending to South and Central American countries that all defaulted at the same time.[142] This was described as an event of "exceptional nature"[143] and thus inconceivable.

Taleb stresses that due to the often slow nature of historical changes and technical implementations that "Black Swans" can be built up over decades (and seemingly gaining credibility with each day of being upheld) but be destroyed within seconds).[144]

Moreover, Taleb rejects the notion of *Knightian* risks (computable risks) and *Knightian* uncertainties (not computable) as he finds them to be "absent from real life" and "mere laboratory contraptions."[145]

To conclude this epistemological[146] reflection on the widely held predictions on the future of warfare, it needs to be emphasized that Taleb's considerations must not necessarily be true and all empiricism based predictions must not necessarily be false.

It was rather the intent of this section to provide one possible explanation of the origin and process of widely shared predictions.

Furthermore, it was the goal of this paragraph to impose some critical reflection on the aura of certainty surrounding many scholars and decision-makers regarding their ability to accurate predict future developments. Undoubtedly, the lessons to be learned from past developments should be crucial factors in determining future defense and security policy for probable events on the horizon. However, it should always be the imperative of defense and security planning to be prepared for the "unlikely" and inconceivable events. This is especially true if the capabilities required for these "improbable" scenarios are very complex and likely to be lost if not practiced on a regular basis or not being assigned sufficient funding.

[132] Id. p. 2.
[133] Id. p. 15.
[134] Id. p.15.
[135] Id., p. 40.
[136] Id., p. 40.
[137] Id. 40: For the sake of accurateness: Russel used a chicken in his original analogy instead of a turkey.
[138] Id. 41.
[139] Id. 41.
[140] As obviously one could make the argument that the experience, the data and number of sources and witnesses in the security policy context are incomparably larger than in the turkey example.
[141] Id. p. IV: Taleb words this as follows: "…A *Black Swan* for the turkey is not a *Black Swan* for the butcher…"
[142] Id. p.43.
[143] Id. p. 43.
[144] Id. p.44.
[145] Id. p.128.
[146] *Epistemology,* STANFORD ENCYCLOPEDIA OF PHILOSOPHY *(*First published Wed Dec 14, 2005), http://plato.stanford.edu/entries/epistemology/ (last visited Feb. 8, 2011).

Fire Down Below: How the Underwear Bomber Revealed the U.S. Counterterrorism Community As Hemmed in by the Seams of Legislative Ambiguity

Braden Civins

On December 25, 2009 a 23-year old Nigerian national boarded Northwest Airlines Flight 253 in Amsterdam, the Netherlands bound for Detroit, Michigan. As the plane neared its final destination, passengers heard sharp popping noises, smelled something acrid, and saw smoke and flames emanating from seat 19A. Umar Farouk Abdulmutallab, his body covered by a blanket, had triggered an explosive device sewn into the hem of his underwear by mixing the chemical Pentaerythritol Tetranitrate (PETN) with Triacetone Triperoxide (TATP), using an acid-filled syringe. Quick-thinking passengers and crewmembers successfully put out the ensuing fire.[1] None of the 289 people aboard Flight 253 sustained serious injuries. Abdulmutallab was detained immediately upon the flight's arrival at Detroit Metropolitan Airport by federal authorities and indicted by a federal grand jury two weeks later.[2]

A preliminary review of the events leading up to the Christmas Day attack conducted by the White House "highlight[ed] human errors and a series of systemic breakdowns" that prevented the detection and disruption of the attack.[3] The review identified several causes for the failure to interdict the plot to bring down Flight 253, but did not specify the degree to which each contributed to the ultimate outcome.[4]

The attack prompted a flurry of congressional hearings. Administration officials' testimony did little to quell Congress's outrage over the failure, and indeed prompted additional questions from congressional members eager to assign fault and uncertain where blame should lie. After all, several months prior to Christmas Day, the counterterrorism (CT) community[5] had collected intelligence that indicated an impending attack of the very type eventually carried out by Abdulmutallab. Moreover, the CT community had fragmentary information that, if collated and understood, would have identified Abdulmutallab's intentions and provided the government ample opportunity to interdict or neutralize the threat.[6] Was this not the exact type of failure that permitted, in part, the attacks of September 11, 2001 to take place? In light of the dramatic overhaul of the intelligence community[7] (IC) undertaken in the wake of 9/11, how is it that the U.S. government's CT apparatus remained so fundamentally flawed as to allow a known radical Islamist with a bomb sewn into his underwear to board a U.S.-bound flight?

Part I of this paper examines the events presaging the Christmas Day attack. Part II explains the complex allocation of authorities and responsibilities among members of the CT community. Part III demonstrates how this confusion affected the handling, processing, and response to critical information provided by Abdulmatallab's father on November 19 and 20, 2009. Part IV considers Congress's post-hoc inquiries, questioning whether the inability to disrupt the plot was justifiably labeled a "failure." Part V provides conclusions and Part VI, recommendations for corrective action.

I. A Brief Look at the Threads of an Under-Handed Plot: The "Dots"

a. Upbringing, Education, and Radicalization

As the son of a wealthy Nigerian banker, Umar Farouk Abdulmutallab demonstrated none of the fundamentalist ardor at a young age that would later motivate his attempt at achieving martyrdom on behalf of al Qaeda in the Arabian Peninsula (AQAP).[8] Like many children of means, he enjoyed basketball and PlayStation.[9] By the time he graduated from the British International School in Lome, Togo in 2004, his views

[1] Scott Shane and Eric Lipton, *Passengers' Quick Action Halted Attack*, N.Y. Times, Dec. 26, 2009, at A1, *available at* http://www.nytimes.com/2009/12/27/us/27plane.html?pagewanted=1&_r=1.

[2] U.S. v. Umar Farouk Abdulmutallab, 2:10-cr-20005-NGE-DAS.

[3] *Summary of the White House Review of the December 25, 2009 Attempted Terrorist Attack*, Jan. 7, 2010 [hereinafter *White House Review*] *available at* http://www.fas.org/irp/news/2010/01/whreview-summary.pdf.

[4] *See id.*

[5] "CT community," for purposes of this study, refers to terrorism-focused components of various government entities, specifically the National Counterterrorism Center in the Office of the Director of National Intelligence, componaents of the Department of State, including consular officials and the Office of the Coordinator for Counterterrorism, and the Central Intelligence Agency's Counterterrorism Center.

[6] As noted by the *White House Review*, *supra* note 3, "[t]he U.S. Government had sufficient information prior to [the attack] to have potentially disrupted the AQAP plot—i.e. by identifying Mr. Abdulmutallab as a likely operative of AQAP and potentially preventing him from boarding flight 253."

[7] The "intelligence community" is ascribed its traditional meaning, and is inclusive of the smaller "CT community." The IC is comprised of 16 government organizations charged with all manner of intelligence collection and analysis, including the Central Intelligence Agency, Defense Intelligence Agency, National Security Agency, National Reconnaissance Office, National Geospatial Intelligence Agency, and the intelligence components of the Armed Forces. Components of the Federal Bureau of Investigation, Department of Homeland Security, the Drug Enforcement Agency, Department of Energy, and Department of Treasury are also members of the IC.

[8] Adam Nossiter, *Lonely Trek to Radicalism for Terror Suspect*, N.Y. Times, Jan. 16, 2010 at A1.

[9] *Id.*

took a decidedly Islamist turn and he began openly advocating the cause of the Taliban.[10] An itinerant student, Abdulmutallab traveled to Yemen in 2005 to study Arabic and, in 2006, studied engineering in London.[11] While he attended mosques kept under surveillance by British security services for their propensity to attract Islamists, he only appeared "on 'the periphery of other investigations' into radical suspects there…he was not considered a terrorist threat himself."[12]

In June 2008, U.S. consular officers in London issued Abdulmutallab a multi-year, multiple-visit tourist visa.[13] This visa was in fact the second U.S. visa Abdulmutallab had obtained. In 2004, a visa request by Abdulmutallab was initially denied after a consular official found false information on his application.[14] However, the consular official's supervisor overturned the denial due to Abdulmutallab's clean record and distinguished family.[15] Since the matter was considered resolved, it was not revisited when the 2008 visa application was made.[16]

In 2008, Abdulmutallab traveled to the United States and Egypt before pursuing a master's degree in international business in Dubai.[17] In May 2009, the British government denied Abdulmutallab's application for renewal of a student visa and placed him on a watch list to prevent him from re-entering Britain.[18] Because the denial was predicated on a fraudulent visa application rather than national security concerns, U.S. officials were not notified of this action despite the fact that Abdulmutallab possessed a U.S. visa at the time. He returned to Yemen in August 2009, ostensibly to resume his studies.[19] Yemeni officials admitted him based on the fact that his passport contained a valid U.S. visa.[20] While there, Abdulmutallab stayed with an AQAP leader for a month, training in preparation for the Christmas Day attack.[21]

b. UNDER SUSPICION: U.S. CT TAKES NOTICE

The individual data points discussed below must necessarily be viewed against the backdrop of the IC's recognition of the threat to U.S. interests posed by AQAP. The IC had "strategic intelligence" that AQAP "had the intention of taking action against the United States prior to…December 25th."[22] Furthermore, the IC "had warned repeatedly of the type of explosive device used by Abdulmutallab and the ways in which it might prove a challenge to screening."[23]

In August 2009, the National Security Agency (NSA) intercepted communications of AQAP leaders in Yemen discussing a terror plot involving a Nigerian.[24] NSA translated and disseminated the information to the National Counterterrorism Center (NCTC). Subsequent intercepts revealed that AQAP was planning an operation for December 25.[25] On November 11, British intelligence officials sent their U.S. counterparts a cable revealing that a man named "Umar Farouk" had spoken to U.S.-born cleric and AQAP affiliate Anwar al-Awlaki and pledged to commit *jihad*, or holy war.[26]

In October 2009, Abdulmutallab sent text messages to his father, Alhaji Umaru Mutallab, professing to have found "real Islam" and insisting that his family forget about him because he had no intention of ever returning to Nigeria.[27] His father, alarmed by his son's ominous tone and espousal of radical ideology, solicited the assistance of Nigerian officials to help him locate his son and persuade him to return home.[28] On November 19 and 20, Alhaji Umaru met with U.S. officials from the Department of State (State) and the Central Intelligence Agency (CIA) at the U.S. Embassy in Abuja, Nigeria.[29] The officials sent memos relating

[10] *Id.*

[11] *Id.* Multimedia graphic entitled *From Student to Terrorism Suspect available at* http://www.nytimes.com/imagepages/2010/01/17/world/17abdu-graphic.html.

[12] *Id.*

[13] Ruth Ellen Wassem, *Immigration: Terrorist Grounds for Exclusion and Removal of Aliens*, 19 CONGRESSIONAL RESEARCH SERVICE (March 2010).

[14] John Solomon, *Visa Denial was Reversed for Terrorism Suspect in 2004*, WASHINGTON POST, March 25, 2010.

[15] *Id.*

[16] *Id.* Furthermore, a State Department spokesman noted that, "there was nothing in his application nor in any database at the time that would indicate the he should not receive a visa," further adding that Abdulmutallab was enrolled at a reputable London university and had ample financial resources. Ian Kelly, *On the Record Briefing,* U.S. Department of State, Washington, D.C., Dec. 28, 2009.

[17] *Lonely Trek to Radicalism*, *supra* note 8.

[18] Russell Goldman and Huma Khan*, Timeline of Terror: Clues in Bomber Umar Farouk Abdulmutallab's Past,* ABC NEWS, Dec. 30, 2009, reporting that Abdulmutallab's application to renew his student visa was denied because he applied to study "life coaching" at a non-existent college.

[19] Mohammed Albasha, Spokesman, Yemeni Embassy to the United States, is interviewed on CNN's "The Situation Room," December 29, 2009.

[20] *Timeline of Terror*, *supra* note 18.

[21] *Id.*

[22] *Aviation Security and Flight 253 before the S. Comm. on Commerce, Science, and Transportation,* 111th Cong. (Jan. 20, 2010) [hereinafter *Aviation Security and Flight 253 Before the S. Comm. on Commerce*] (statement of Michael Leiter, Director of NCTC).

[23] *Id.* AQAP had carried out an attack on a Senior Saudi CT official two months prior to Christmas Day in which a suicide bomber detonated PETN that was similarly sewn into his underwear. Although the attack did not achieve its objective, the PETN successfully detonated, killing the AQAP operative. Also, on Nov. 11, 2009, a Somali man was arrested trying to board a commercial airliner in Mogadishu carrying a syringe and explosives in his underwear – a homemade explosive device similar to the one Abdulmutallab was carrying on Christmas Day. *Timeline of Terror, supra* note 18.

[24] *Early Leads Before the Attack*, *supra* note 11.

[25] Eric Lipton, Eric Schmitt, and Mark Mazzetti, *Review of Jet Bomb Plot Shows More Missed Clues*, N.Y. TIMES, Jan. 17, 2010 at A1.

[26] *Detroit Bomber Cooperating with the FBI*, THE NATIONAL (UAE), Feb. 5, 2010, *available at* http://www.thenational.ae/news/worldwide/americas/detroit-bomber-co-operating-with-fbi.

[27] *Lonely Trek to Radicalism*, *supra* note 8.

[28] *Id.*

[29] Mark Mazzetti and Eric Lipton, *Spy Agencies Failed to Collate Clues on Terror*, N.Y. TIMES, Dec. 31, 2009, at A1.

general details of the meeting to designated components of the intelligence and law enforcement communities, including NCTC.[30] CIA then compiled biographical data on Abdulmutallab but did not share his profile with NCTC or other members of the IC.[31]

NCTC entered Abdulmutallab's name into the Terrorist Information Datamart Environment (TIDE), the largest terrorist watchlist, which contained the names of 550,000 people with potential ties to terrorist organizations. NCTC analysts, as a result of inadequate information on Abdulmutallab, decided not to nominate him for inclusion in the smaller, more refined watchlists that would have resulted in additional scrutiny at airport checkpoints or denial of entry to board a U.S.-bound flight.

c. Caught With Our Pants Down: Abdulmutallab Flies Wide Open

On December 16, an unidentified individual in Accra, Ghana paid cash for Abdulmutallab's round-trip plane ticket to Detroit, Michigan. On the day of his flight Abdulmutallab did not check any luggage.[32] Boarding Flight 253 in Amsterdam on December 25, Abdulmutallab was not subjected to any secondary passenger screening. Department of Homeland Security (DHS) officials received a routine electronic notice of Abdulmutallab's airline reservation—which may have included details about the cash payment to purchase his ticket and his lack of baggage.[33] During the eight-hour flight from Amsterdam to Detroit, Customs and Border Patrol (CBP) officers discovered that Abdulmutallab was listed in the TIDE database and decided to question him immediately upon his arrival.[34]

II. The Legislative Underpinnings of the CT Community: The Loose Elastic Holding It All Together

a. Intelligence Reform: Readjusting the Constrictive Fabric of the IC

The CT community had fragmentary intelligence regarding the Christmas Day plot that, if properly collated and understood, would have resulted in Abdulmutallab's nomination to a visa screening "lookout" list and border inspection list.[35] By late November several "dots" of information had been collected from different components of the IC: (1) strategic intelligence that AQAP posed a "growing threat to US interests" in the Arabian Peninsula;[36] (2) analysis indicating the possibility of AQAP directing attacks against the U.S. homeland;[37] (3) indications that PETN was becoming the weapon of choice for AQAP operations; (4) signals intercepts indicating AQAP was recruiting a Nigerian national for a future operation; (5) a cable indicating an "Umar Farouk" had met with known AQAP affiliate Anwar al-Awlaki; (6) and the information collected by State and CIA at the Abuja Embassy suggesting that Abdulmutallab had fallen in with extremists in Yemen. Administration officials later claimed the failure to detect and interdict Abdulmutallab did not result from inadequate information sharing among the CT community. Congressional testimony by NCTC officials echo and amplify this assertion, suggesting that NCTC and, perhaps, CIA all-source intelligence analysts had access to all of the intelligence described above.

Enjoying the benefit of 20/20 hindsight, some in Congress argued, given the wealth of available information on Abdulmutallab prior to the attack, the near success of the Christmas Day plot marked a clear failure on the part of the CT community. In congressional hearings, CT officials met with countless variations of the same basic query: what went wrong? Explanations offered by CT officials as to why the information was not collated reveal deficiencies in the analytic process, shortfalls in IC resource allocation and, most troubling of all, continued confusion as to the authorities, responsibilities, and functions of the various members of the CT community.

Prior to 9/11, the many databases of IC agencies were disjointed and lacked interoperability. Stovepiping, or the tendency of agencies to husband information, combined with the "wall" separating law enforcement investigations and intelligence operations, prevented authorities from watchlisting at least two 9/11 hijackers who were known to various law enforcement and intelligence authorities.[38] The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)[39] sought to break down many of the barriers hindering interagency cooperation through the establishment of an organization designed to serve as a single hub for all international terrorist threat information. IRTPA established NCTC and designated it the "primary organization…for analyzing and integrating all intelligence possessed or acquired…pertaining to terrorism and counterterrorism, excepting intelligence pertaining exclusively to domestic terrorists and domestic counterterrorism."[40] NCTC, placed under the

---

[30] *Id.*
[31] *Id.*
[32] *Early Leads Before the Attack*, *supra* note 11.
[33] Mark Randol, *The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress*, 24 CONGRESSIONAL RESEARCH SERVICE (March 2010).
[34] *Id.*
[35] *Sharing and Analyzing Information to Prevent Terrorism Before the H. Comm. on the Judiciary*, 111th Cong. (March 24, 2010) [hereinafter *Sharing and Analyzing Information Before the H. Judiciary Comm.*] (statement of Russell Travers, Deputy Director for Information Sharing and Knowledge Development, NCTC).
[36] *Intelligence Reform: The Lessons and Implications of the Christmas Day Attack, Part I Before the S. Comm. On Homeland Security and Governmental Affairs*, 111th Cong. (Jan. 20, 2010) [hereinafter *Lessons and Implications, Part I Before the S. Homeland Security Comm.*] (statement of the Hon. Dennis Blair, Director of National Intelligence).
[37] *Id.*
[38] *See National Commission on Terrorist Attacks Upon the United States*, *The 9/11 Commission Report* 254-66 (New York: W.W. Norton & Company, 2004) [hereinafter *9/11 Commission Report*].
[39] IRTPA, P.L. 108-458, 118 Stat. 3638 (enacted Dec. 17, 2004).
[40] *Id.* Subtitle B, Sec. 1021(d)(1); codified at 50 USC § 404o(d)(1).

authority of the Director of National Intelligence (DNI), is tasked with serving "as the central and shared knowledge bank on known and suspected terrorists and international terror groups."[41]

Even with NCTC's tasking, no member of the CT community has been forced to eliminate its analytic components that receive and analyze information related to terrorism. On the contrary, although NCTC is the primary mechanism for the analysis and synthesis of international terrorism-related information, CIA continues to conduct its own all-source analysis with capabilities and methods discrete from those of NCTC.[42] This intentional redundancy serves to "layer" the analytic process and hedge against the possibility of critical information falling through interagency gaps.[43]

b. NCTC's Directorate of Intelligence: Under-equipped, Under-staffed, and Under-resourced

With primary responsibility for the analysis of all international terrorism-related information and a statutory position at the heart of the IC, NCTC's Directorate of Intelligence (DI) bears the burden for the "failure" to make sense of the fragmentary information concerning Abdulmutallab. Several possible explanations shed light on why NCTC, at least in the view of Congress, came up short. As a general matter, improving intelligence collection has long been the focus of the IC, with intelligence analysis historically regarded as a secondary priority.[44] The incredibly high volume of intelligence received by NCTC's DI on a daily basis requires cutting-edge technology and a well-resourced staff to process and analyze information intake. NCTC's DI receives and reviews around five thousand pieces of CT intelligence on a daily basis, often implicating thousands of identities.[45] Partial names and different spellings hinder NCTC's ability to draw linkages from the data.[46] In 2009 alone, NCTC received 3,000 Visas Viper cables, the type of transmittal sent by consular officials to NCTC as a result of the meetings with Alhaji Umaru in the Abuja Embassy.[47]

NCTC officials insisted that the two Visas Viper cables, discussed in Part IIIA, sent to NCTC as a result of the Abuja meetings "existed largely 'in the noise,' and there was simply nothing particularly alerting about either 'dot.'"[48] While Congress expressed dismay over NCTC's inability to separate the wheat from the chaff given what was known about Abdulmutallab, NCTC officials' testimony suggests that, given the volume of intelligence monitored by NCTC and the absence of a single piece of derogatory data suggesting Abdulmutallab posed a serious threat, the inability to collate pertinent data was not an aberration. Piecing together fragmentary information is "a very complicated challenge involving both numbers of analysts and the use of technology to correlate vast amounts of information housed in multiple agencies and systems."[49] NCTC officials acknowledged that technological progress was needed to improve intelligence analysis;[50] however, technological improvement alone is not a panacea for curing the deficiencies of the analytic process.

Understaffing was also a critical part of the equation, with NCTC operating with around 600 analysts when the Christmas Day attack occurred.[51] As NCTC Director Michael E. Leiter noted in congressional testimony, "we simply need the people to do [the analysis], because you can have the best Google-like tool in the world [but]…the people to work that watch list and look at that information [are still necessary]."[52] NCTC did not have the manpower to sift through and analyze all available data, which would explain in part why "NCTC…personnel who are responsible for watchlisting did not search all available databases to uncover additional derogatory information that could have been correlated with Abdulmutallab."[53] The White

---

[41] *Id.* Subtitle B, Sec. 1021(d)(6); codified at 50 USC § 404o(d)(6).

[42] In accordance with statute, CIA maintains the responsibility and resource capability to "correlate and evaluate intelligence related to national security and provide appropriate dissemination of such intelligence." 50 U.S.C. § 403-4a(d)(2).

[43] As NCTC Director Leiter noted in testimony, "Also with responsibility, pursuant to the president's conclusions and consistent with past practice, was the CIA. We both had responsibility to [collate the available data on Abdulmutallab]." *Aviation Security and Flight 253 Before the S. Comm. on Commerce*, *supra* note 22 (testimony of Michael Leiter, Director of NCTC). At the same hearing, the Hon. Lee Hamilton described the benefit of this redundancy, stating:

> Redundancy doesn't bother me particularly, because if you got the CIA doing analytical work on the threat and the NCTC, that's OK, because the thing that impresses me about the analyst is the work can be boring -- I mean really boring, sorting through massive amounts of data and trying to figure out what's right there or what's significant. And somebody's going to be asleep at the switch now and then, so some redundancy doesn't bother me.

[44] Intelligence Reform: The Lessons and Implications of the Christmas Day Attack, Part II *Before the S. Comm. on Homeland Security and Governmental Affairs*, 111th Cong. (Jan. 26, 2010) (testimony of Lee Hamilton, Chair of the 9/11 Commission, stating "The collection side we're -- we're very good at; the analyst side less good at. And I think the reason for it is because we simply haven't given it the priority it deserves").

[45] *Sharing and Analyzing Information Before the H. Judiciary Comm.*, *supra* note 35 (statement of Russell Travers, NCTC).

[46] *Id.*

[47] Wassem, *Immigration: Terrorist Grounds for Exclusion*, *supra* note 13.

[48] *Sharing and Analyzing Information Before the H. Judiciary Comm.*, *supra* note 35 (testimony of Russell Travers, NCTC).

[49] *Id.*

[50] *Aviation Security and Flight 253 Before the S. Comm. on Commerce, supra* note 22 (in testimony, NCTC Director Leiter asked, "Do we have the systems in place that make it easy to connect those pieces of data in the first instance? And the answer is yes in some places and not nearly enough so in others. Some agencies are far ahead of others. And we still have clearly some systems which are so rudimentary and basic, that they're not doing a good job of that").

[51] Richard Best, *The National Counterterrorism Center (NCTC)—Responsibilities and Potential Congressional Concerns*, at 4 Congressional Research Service (Jan. 15, 2010).

[52] *Aviation Security and Flight 253 Before the S. Comm. on Commerce, supra* note 22 (statement by Michael Leiter, Director of NCTC).

[53] *White House Review*, *supra* note 3; *see also supra* note 51 (offering a discussion of analytic responsibilities among the IC).

House Review found that one of the "failures" of the CT community was that "[IC] leadership did not increase analytic resources working on the full AQAP threat." If the Review's finding was referring to NCTC, the term "failure" was a mischaracterization: NCTC does not possess direct authority over either its budget or staffing.[54] The issue of inadequate resource allocation is a symptom of a more fundamental deficiency in the 2004 intelligence reform legislation that is further evidenced, if not epitomized, by NCTC's Directorate of Strategic Operational Planning.

c. NCTC's Directorate of Strategic Operational Planning: Jockeying for Relevance in the CT Community

We therefore propose a new institution: a civilian-led unified joint command for counterterrorism. It should combine strategic intelligence and *joint* operational planning [emphasis added].[55] *– 9/11 Commission Report*

The White House Review found that one of the primary explanations for the "failure" to detect the Christmas Day plot was that no CT entity took responsibility for "running down" the threat streams emanating from AQAP.[56] According to the President, "the intelligence community did not aggressively follow up on and prioritize particular streams of intelligence related to a possible attack against the homeland."[57] NCTC Director Leiter acknowledged that, by presidential instruction, NCTC bears primary responsibility "to ensure a system of…follow-up of high priority threats."[58] The White House Review, however, did not explicitly blame this failure on NCTC, stating only that, "[n]o single component of the CT community assumed responsibility for the threat reporting."[59]

The White House's reluctance to pin this responsibility on any one actor is telling—not because the White House was trying to avoid taking ownership of the "failure" for the sake of political expediency, but rather because of the uncertainty, codified in statute, as to where responsibility for following up on threats should lie. NCTC is only capable of conducting follow-up by developing analytic resources devoted to focusing on specific pieces of information. Although the Office of the DNI (ODNI) has authority to task members of the IC with collecting additional information on specified targets, NCTC does not have derivative tasking authority by virtue of being within ODNI. Information flow between NCTC and the rest of the CT community is decidedly one-way. Bearing that in mind, NCTC Director Leiter's testimony before a congressional committee investigating the attack on Flight 253 merits scrutiny. Leiter discussed the possibility of NCTC conducting operational follow-up when more information is needed on a particular threat stream. He implied NCTC should assert more authority over the process, claiming operational follow-up could be conducted through a system whereby NCTC identifies threats and tasks an agency with taking further investigative action. It was unclear whether Congress was receptive to the NCTC Director's implicit request for a measure of authority over the tasking process.[60] NCTC's lack of tasking authority might have been a moot point with respect to the Christmas Day plot, as no publicly available information suggests any IC agency tasked additional collection after receiving information on Abdulmutallab.

An examination of NCTC's authority, or lack thereof, to conduct operations offers insight into the depth of confusion surrounding NCTC's role in the CT community. IRTPA expressly prohibits the NCTC Director from "direct[ing] the execution of counterterrorism operations."[61] Although the scope of activity falling within the definition of "CT operations" is uncertain, it likely entails operations intended to collect additional "dots" of information. Testifying before Congress following the Christmas Day attack, Leiter did not seek any amendment to this prohibition.[62] While this prohibition and Leiter's acceptance of it are unremarkable, they raise a perplexing question: just what is NCTC's Directorate of Strategic Operational Planning?

One of NCTC's primary missions is "to conduct strategic operational planning for counterterrorism activities, integrating all instruments of national power…within and among agencies."[63] IRTPA

[54] The NCTC Director is completely reliant upon the Director of National Intelligence for determining budgetary allocations and policy with respect to personnel. NCTC's budget is comparatively modest among members of the IC, and most NCTC spending goes to covering personnel expenses. *NCTC—Responsibilities and Potential Concerns*, *supra* note 51, at 9.

[55] *9/11 Commission Report*, at 403, *supra* note 38.

[56] *White House Review*, *supra* note 3 (finding that there was a "failure within the CT community, starting with established rules and protocols, to assign responsibility and accountability for follow up of high priority threat streams, run down all leads, and track them through to completion").

[57] *President Obama's Remarks on Security Review of Attempted Terrorist Attack on Christmas Day* (Jan. 7, 2010).

[58] *Aviation Security and Flight 253 Before the S. Comm. on Commerce, supra* note 22 (statement by Michael Leiter, Director of NCTC).

[59] *White House Review*, *supra* note 3.

[60] *Aviation Security and Flight 253 Before the S. Comm. on Commerce, supra* note 22. NCTC Director Leiter said, "at least we will establish a system whereby each of these threats, when we identify threats, can, in fact, be followed up through appropriate department or agency action. And the results of that follow-up are reported back to the [NSC] to ensure that they have the information they need to further direct action as necessary." Leiter acknowledged that, as constituted, NCTC does not have the tasking authority he describes in terms of follow-up investigations: "I do not [have], nor do I believe the DNI as currently constructed has, all of the authorities to move all of the information in a way that will maximize the likelihood of detecting these plots." Although the DNI possesses tasking authorities, many commentators suggest that authority is not transmitted to NCTC which, in effect, had no such authority prior to the Christmas Day attack. See Marc Armbinder, *The Leiter They Are, the Quicker They Fall*, THE ATLANTIC (Jan. 7, 2010), *available at* http://www.theatlantic.com/politics/archive/2010/01/the-leiter-they-are-the-quicker-they-fall/33118/.

[61] IRTPA, P.L. 108-458, Section 1021, Sec. 119(g).

[62] *Aviation Security and Flight 253 Before the S. Comm. on Commerce, supra* note 22 (statement by Michael Leiter, Director of NCTC).

[63] 50 USCS § 404o(d)(2).

established the nominally contradictive[64] Directorate of Strategic Operational Planning (DSOP) to accomplish this end. DSOP was chartered "to provide the 'connective tissue' between national counterterrorism policy and strategy established by the President, normally via the National Security Council system, and counterterrorism operations conducted by the departments and agencies."[65] In theory, DSOP coordinates along both vertical and horizontal lines: it receives policy guidance from the NSC and, through an interagency process, "assign[s]…roles and responsibilities"[66] to various CT agencies to implement the policy at an operational level. Assuming DSOP performs the functions ascribed to it by statute, the threat posed by Abdulmutallab would fall within DSOP's purview.[67]

In reality, had NCTC analysts pieced together the available information on Abdulmutallab, it is unlikely DSOP would have been able to coordinate any operational response to the identified threat. A report issued in February 2010 by the Project on National Security Reform (PNSR) identified several "systemic impediments" that undercut DSOP's ability to effect either strategic or operational planning, including: overlapping authorities among CT entities; inadequate congressional understanding of DSOP's mission and insufficient oversight of its activities; and inadequate means available to DSOP for "prioritiz[ing] resources and investments in capabilities for complex, multidimensional [CT] missions."[68] Two interrelated issues raised by PNSR are important to understanding the foundational flaws in the CT community that allowed Abdulmutallab to slip through the cracks: (1) the overlapping authorities among NCTC, State, and CIA; and (2) the institutional tensions inhibiting DSOP from managing collaborative interagency CT operations.

As noted earlier, the NCTC Director is prohibited by statute from executing CT operations, leaving that responsibility to individual agencies. Although the 9/11 Commission recommended that NCTC be "given the authority of planning the activities of other agencies," the Commission did not specify the scope of this authority,[69] and IRTPA, although largely implementing the 9/11 Commission's recommendations regarding NCTC, refrained from granting DSOP this unprecedented power.[70] IRTPA also required the president to issue guidance to the DNI to implement reform "in a manner that respects and does not abrogate the statutory responsibilities of the heads" of other IC agencies.[71]

So, although DSOP was tasked with providing strategic operational plans for CT operations, which includes coordinating operational activities among agencies, assigning roles and responsibilities, and monitoring plans' implementation, it was given no "'hammer' authority to compel agencies to align their plans and activities, or to fulfill their roles and responsibilities under strategic operational plans."[72] Nor was NCTC given the budgetary control necessary to encourage interagency buy-in—the NCTC Director possesses only the ability to advise the DNI on "the extent to which counterterrorism recommendations and budget proposals of departments, agencies and elements of the United States government conform to the priorities established by the president."[73]

DSOP, as a component of NCTC, lacks even the authority to determine "which personnel or specific capabilities should be utilized by agencies in mission execution."[74] Existing mechanisms to ensure participation in the interagency strategic operational planning process at DSOP are weak,[75] and DSOP has been reluctant to aggressively use what authority it has, preferring instead to rely on the willingness of other agencies to support DSOP's mission. When DSOP attempts to exercise its authority, CIA and State tend to resist what they view as DSOP's encroachment, using the statutory vagueness of "strategic operational planning" as a means to block DSOP's efforts to live up to its statutory mandate. As one NCTC official put it:

> If you started to do an operational plan they would say, "That's too operational, that's too tactical. You're supposed to be focused more on strategic." If we trended toward the strategic they would say,

[64] PROJECT ON NATIONAL SECURITY REFORM, TOWARD INTEGRATING COMPLEX NATIONAL MISSIONS: LESSONS FROM THE NATIONAL COUNTERTERRORISM CENTER'S DIRECTORATE OF STRATEGIC OPERATIONAL PLANNING, (Feb. 2010) at 47-51 [hereinafter referred to as PNSR REPORT] (explaining that the term "joint operational planning" was the source of contentious debate, as it implied the allocation of too much authority to the DSOP—the compromise language, "strategic operational planning," beyond its contradiction in terms, has become a point of consternation for those in the DSOP).

[65] *Id.* at XI.

[66] 50 USCS § 404o(d)(3).

[67] According to a statement by Leiter, NCTC is "intended to be a one stop shop for mapping out the terrorism threat and designing a plan for the U.S. Government to counter it—whether it is immediate, emerging, or long-term." *Looming Challenges in the War on Terror, Remarks by Michael Leiter to the Washington Institute*, Feb. 13, 2008. *See also* PNSR REPORT (stating that, "[DSOP] was proposed to translate counterterrorism policy and strategy into strategic and operational interagency plans that range from broad objectives to specific tasks and from the long term to the immediate") at 49.

[68] PNSR REPORT at XV, *supra* note 64.

[69] *See 9/11 Commission Report* at 406, *supra* note 38.

[70] PNSR REPORT at 33, *supra* note 64 (granting NCTC that authority was considered "unprecedented" by PNSR because few, if any, government agencies in the history of the U.S. government have had the ability to cut through the normal bureaucratic hindrances common to all interagency processes).

[71] IRTPA 2004, P.L. 108-458, Title I, Subtitle A, § 1018, 118 Stat. 3670 (effective not later than six months after enactment, as provided by § 1097 of such Act, which appears as 50 USCS § 401 note); *see also* The Lessons and Implications of the Christmas Day Attack: Intelligence Reform and Interagency Integration *Before the S. Comm. on Homeland Security and Governmental Affairs*, 111th Cong. (March 17, 2010) (testimony of the Hon. Benjamin Powell, Former General Counsel to DNI, stating "[t]he goal is not to diminish the authorities or the capabilities of one organization in favor of another organization such as the DNI. The goal is to have an integrated intelligence community that is more than the sum of its parts").

[72] PNSR REPORT at 38, *supra* note 64.

[73] Codified at 50 USCS § 404o(f)(C).

[74] PNSR REPORT at 47, *supra* note 64 (quoting NCTC Director Michael Leiter's testimony before the House Committee on Homeland Security on Oct. 4, 2007).

[75] *Id.* at 113.

"No, you should be more focused on the operational.[76]

Interagency involvement in strategic operational planning is entirely voluntary, with DSOP relegated to facilitating interagency cooperation and coordination rather than forcibly ensuring that it occurs.[77] As Leiter explained in testimony, "we've become a negotiator and mediator of sorts, rather than a director of action."[78] Leiter likely overstates the case, as other testimony suggests NCTC's lack of authority leaves it largely unable to perform even this arbitration function effectively.[79] An examination of the authorities, culture, and institutional interests of State and CIA with respect to CT reveal very little incentive for either entity to invest in DSOP-led processes.

d. Stitched Together: Tracing the Seams of Authority and Function Among NCTC, State, and CIA

State's Office for Combating Terrorism was established in 1972, following the attack by Black September, a radical Palestinian terrorist organization, on Israeli athletes at the Munich Olympics. As the PNSR report notes, "it has always (nominally) been the primary entity within the U.S. government responsible for managing international terrorist incidents and programs."[80] By statute, State's Office of the Coordinator for Counterterrorism (State/CT), as it has come to be known, is charged with providing "overall supervision (including policy oversight of resources) of international counterterrorism activities."[81] Like the NCTC Director, the Coordinator was given no "hammer" to compel operational activities by other departments and agencies or ensure compliance with CT objectives set forth by State. State/CT views itself as the leader of U.S. government CT efforts, and its mission statement is laid out in terms strikingly similar to those of DSOP as prescribed by IRTPA.[82] It is therefore no surprise that DSOP planning processes often lack participation by State personnel. It is also no surprise that the PNSR found that, "ambiguous delineation of roles and responsibilities has resulted in duplication of effort and inefficiency" between State and NCTC.[83]

While consular officials at the Abuja Embassy followed protocol by notifying NCTC of the meeting with Abdulmutallab's father, various claims by State officials suggest CIA, rather than NCTC, called the shots in any subsequent operational planning that occurred with respect to Abdulmutallab. Given the nebulous lines of authority and responsibility among State, NCTC, and CIA, the State officials who were privy to the information provided by Alhaji Umaru were justified in pursuing one of three routes in terms of operational response: (1) deferring to NCTC to formulate a plan for running the threat to the ground; (2) deferring to CIA; or (3) assuming operational responsibility.[84] In light of the existing collaborative relationship between State and CIA in responding to international terrorism threats, strengthened by a history of mutual cooperation, it is likely standard practice for State to defer to CIA to address the type of threat posed by Abdulmutallab. The State-CIA relationship tends to further exclude NCTC from exerting any influence on CT operational planning.

CIA's broad authority to conduct international operations relating to national security, codified in the "fifth function" of its legislative framework, has put international terrorism in its crosshairs at least as far back as 1972.[85] Although CIA's Counterterrorism Center (CTC) was only established in 1986 following the marine barracks bombing in Lebanon, CIA had, since 1947, enjoyed premier status in the IC and served as the primary agency for combating all manner of international threats to the U.S. With its own all-source intelligence collection and paramilitary capabilities, CIA

---

[76] *The Lessons and Implications of the Christmas Day Attack: Intelligence Reform and Interagency Integration Before the S. Comm. on Homeland Security and Governmental Affairs*, *supra* note 71 (testimony of Richard Nelson, former DSOP official).

[77] PNSR Report at 70, *supra* note 64 (Kevin Brock, former Principal Deputy Director at NCTC, clarified this role by stating, "NCTC is not directing operations…. We're here just to kind of act as the air traffic controller and make sure everyone is talking"). Furthermore, DSOP has tended not use its authorities robustly and risk alienating its interagency partners and has favored a strategy of maintaining a "coalition of the willing." For example, DSOP has traditionally tended to shy away from any assessment that holds departments and agencies accountable for fulfillment of certain objectives. While DSOP has the authority to assign roles and responsibilities and monitor department and agency implementation of strategic operational planning, there have been instances where departments and agencies did not participate in the planning process, implement DSOP's strategic operational plans, or even perform the roles and responsibilities assigned to it.

[78] *Intelligence Reform, Part I Before the S. Comm. on Homeland Security and Governmental Affairs*, *supra* note 12 (testimony by NCTC Director Michael Leiter).

[79] Richard Nelson testified, "Somebody should be arbitrating…decisions at a much lower level. And that's a role that NCTC could take -- undertake, but it can't do because it doesn't have the credibility and the authority currently to do that." *The Lessons and Implications of the Christmas Day Attack: Intelligence Reform and Interagency Integration Before the S. Comm. on Homeland Security*, *supra* note 71.

[80] PNSR Report at 116, *supra* note 64.

[81] P.L. 105-227 [H.R. 4328].

[82] Compare State/CT's mission statement, to develop and lead "a worldwide effort to combat terrorism using all the instruments of statecraft: diplomacy, economic power, intelligence, law enforcement, and military," and providing "foreign policy oversight and guidance to all U.S. Government international counterterrorism activities" with that of DSOP, which is "to conduct strategic operational planning for CT activities, integrating all instruments of national power, including diplomatic, financial, military, intelligence, homeland security, and law enforcement activities within and among agencies." PNSR Report at 117, *supra* note 64.

[83] *Id.*

[84] While unilateral responsive action by State might seem far-fetched with CIA case officers close at hand in U.S. embassies in consulates worldwide, State's Diplomatic Security Service does play a role in CT investigations abroad.

[85] The "fifth function," originally set forth in the National Security Act of 1947, Pub. L. No. 80-253, 61 Stat. 495, refers to CIA's statutory responsibility to "perform such other functions and duties related to intelligence affecting the national security as the President or the Director of National Intelligence may direct…". 50 USC §403-404(a).

enjoyed de facto authority in addressing international terrorism prior to IRTPA's passage in 2004. If an organization's "role in the CT mission is informed by the organization's history, culture, and leadership…codified by statutes and Executive Orders,"[86] it should come as no great shock that CIA has been indisposed to submitting its resources and personnel to the planning activities of a newly-minted and ill-defined interagency planning process. The PNSR report describes one telling episode when a DSOP-drafted plan was roundly criticized for not incorporating input from CIA. However, as CIA had not participated in the planning process and DSOP, reluctant to engage in a turf war with such a formidable and well-established agency,[87] did not attempt to solicit CIA's involvement, it is "no surprise that [CIA's] perspectives were not fully considered."[88]

Following the meetings between Embassy-based CIA operations officers and Abdulmutallab's father on November 19 and 20, CIA analysts compiled biographical data on Abdulmutallab. As noted in Part II, this information was not shared with NCTC. This information sharing failure was attributed to the mere oversight of one office within CIA; it was not regarded as symptomatic evidence of underlying confusion regarding proper authorities in CT operations.[89]

DSOP, although nominally charged with serving a similar function to State/CT and CTC, lacks the authority, budget, and institutional legitimacy of the other entities. DSOP has no mechanism to control any constituent part of the CT community, and therefore no means by which to hold departments and agencies accountable for missteps. Personnel from CT agencies serving in rotation at NCTC remain beholden to their respective agencies.[90] Serving at DSOP, like many interagency posts, offers little chance for advancement. There is, to put it mildly, little incentive for the CT community to buy into DSOP's interagency processes.

Even when NCTC has attempted to assign roles and responsibilities in CT operations, CT entities have refused to accept NCTC's delegation. All CT entities, including those in State, CIA, and the Department of Defense (DoD) possess the authority to plan and execute CT operations.[91] The current structure is woefully inefficient: "[t]he counterterrorism system is a spider web of overlapping missions, conflicting cultures, and ambiguous lines of authority…this diffusion of responsibility and accountability leads to ineffective management of the mission."[92] A former DSOP official, referring to the coordination of CT activities, offers a frank assessment of the current state of the CT community, noting, "the [IC] and, arguably the government as a whole, still lacks a truly interactive process for addressing terrorism."[93]

In discussing NCTC authorities during a congressional hearing, NCTC Director Leiter noted that the statutory language ostensibly placing NCTC in charge of CT operations was left "purposefully vague."[94] Perhaps this vagueness was an effort to provide the CT community flexibility and leeway to adapt to the fluid and dynamic threat posed by international terrorism. Statements by 9/11 Commission Chairman Lee Hamilton and Senator Susan Collins suggest that, while statutory vagueness exists, the more pertinent issue is the unwillingness of those officials in offices created by IRTPA to exercise existing authorities.[95] It is interesting to note, however, Hamilton's admonition that NCTC should not be given tasking authority to assign roles and responsibilities for conducting follow-up investigations.[96] The fact that Hamilton, a co-author of the 9/11 Commission Report, makes somewhat inconsistent claims about what NCTC's authorities and responsibilities should be may simply reflect his acknowledgment of the laborious horse-trading inherent in pursuing further reform. IRTPA was hard enough to pass; perhaps it is best to leave well enough alone. Senator Collins has expressed similar concerns. Acknowledging the messiness of the initial legislative process, she recalled how §1018 of IRTPA, prohibiting "abrogat[ion]" of existing agency and department authorities, was the result of a compromise without which the House Armed Services Committee would have killed the entire intelligence reform bill.[97] Senator Joseph Lieberman's colorful use of metaphor to describe the deliberative process preceding passage of IRTPA amplified this point:

---

[86] PNSR REPORT at 113, *supra* note 64.

[87] NCTC's reluctance to assert its influence on CT operations, some critics maintain, is commonplace. One report notes that NCTC has demonstrated "a seeming unwillingness to take a bold implementation approach and a preference to avoid bureaucratic conflict." Brian R. Reinwald, *Assessing the National Counterterrorism Center's Effectiveness in the global War on Terror,* U.S. ARMY WAR COLLEGE (Carlisle Barracks, Pennsylvania) (2007).

[88] PNSR REPORT at 115, *supra* note 64.

[89] *Aviation Security and Flight 253 Before the S. Comm. on Commerce*, *supra* note 22 (statement of Michael Leiter, Director of NCTC).

[90] One critic of NCTC notes that it "sustains an environment that fosters continued loyalty of NCTC employees to their parent agencies rather than the NCTC itself." Brian R. Reinwald, *Assessing the National Counterterrorism Center's Effectiveness in the global War on Terror, supra* note 87.

[91] Title X, USC.

[92] PNSR REPORT at 113, *supra* note 64.

[93] The Lessons and Implications of the Christmas Day Attack: Intelligence Reform and Interagency Integration *Before the S. Comm. on Homeland Security and Governmental Affairs*, *supra* note 71 (testimony of Richard Nelson, former DSOP official).

[94] *Aviation Security and Flight 253 Before the S. Comm. on Commerce, supra* note 22 (statement of Michael Leiter, Director of NCTC).

[95] *Intelligence Reform: The Lessons and Implications of the Christmas Day Attack, Part II Before the S. Comm. On Homeland Security and Governmental Affairs*, *supra* note 44 (testimony of Lee Hamilton, former co-chair, 9/11 Commission, stating, "I think there probably are some ambiguities in the law, although you can argue, as I think Senator Collins was doing in her opening statement, that it's more a failure of exercising authority that ambiguity").

[96] *Id.* Hamilton testified, "I don't think that's the role of the NCTC. I -- I am not quite sure where -- where that responsibility lies, but the assignment of responsibility to investigate and to pursue a suspect has to be very clear."

[97] The Christmas Day Attack: Intelligence Reform and Interagency Integration *Before the S. Comm. on Homeland Security and Governmental Affairs*, *supra* note 71.

> I can remember the debates, the extensive debates about the various terms that we put into the 9/11 legislation. And it's seems as if -- but not quite as neat, that we were architects or construction management operation deciding how best to build a building. They're not as neat because there was [sic] more interests at the table than the design and construction teams. Because in some sense, the people at the table wanted to preserve the existing parts of their building.[98]

Whatever the reason for legislative ambiguity, its ultimate effect is to obscure lines of accountability and responsibility, thereby hindering oversight and support of the CT community. Despite the Administration's insistence that the CT community's "failures" preceding the Christmas Day plot are distinct from those preceding the attacks on 9/11, the conclusions of the 9/11 Commission Report are unsettlingly applicable to the more recent case. The 9/11 Commission correctly concluded that the inability of CT entities to conduct joint action, share information, and connect the dots were only symptoms of a larger disease plaguing the CT community. The more fundamental problem, which IRTPA was specifically intended to address, was that:

> [N]o one was firmly in charge of managing the case and able to draw relevant intelligence from anywhere in the government, assign responsibilities across the agencies…track progress, and quickly bring obstacles up to the level where they could be resolved. Responsibility and accountability were diffuse.[99]

As the individual components of the CT community "interpret their [CT] responsibilities largely based on their individual statutes, histories, bureaucratic cultures, and current leadership,"[100] Congress's histrionic finger-pointing following the Christmas Day attack seems profoundly misguided. Rather than forcing CT officials to offer platitudes and reassurances that no such mistakes will be made in the future, congressional inquiry should reexamine the underlying framework of the CT community. Evidence of its debilitating effects on CT efforts was laid bare by the CT community's response to the information provided by Abdulmutallab's father in Abuja.

III. UNDER-INTEGRATION IN PRACTICE: HOW AN UNSTABLE LEGISLATIVE FOUNDATION PLAYS OUT AT THE OPERATIONAL LEVEL

A. THE U.S. DEPARTMENT OF STATE AS THE OUTER GARMENT OF THE CT COMMUNITY: THE ABUJA MEETING

Alhaji Umaru Mutallab, upon receiving unsettling text messages from his son described in Part I, visited the U.S. Embassy in Abuja, Nigeria on November 19 and 20 to seek help. On November 20, the Embassy sent a cable to NCTC providing a general overview of the discussions with Alhaji through the Visas Viper system, the standard form of interagency communication for screening suspected terrorists.[101] The memo read, "Information at post suggests [that Farouk] may be involved in Yemeni-based extremists."[102] However, a consular officer misspelled Abdulmutallab's name when conducting a name check in the State's Consolidated Consular Database (CCD), a resource available to all embassies and consulates containing the names of current U.S. visa holders. As a result of the misspelling, the Visas Viper cable did not indicate that Abdulmutallab held a visa.[103] On November 25, an amended cable containing the correct spelling was sent to NCTC—however, for reasons that remain unclear, the second cable was sent from "another [State] source" in the Embassy, and Abdulmutallab's visa status was not checked prior to sending the amended cable.[104] NCTC was not notified of Abdulmutallab's status as a visa holder.

A short time after the initial Visas Viper cable was sent, Abdulmutallab's name was entered into the Consular Lookout and Support System (CLASS), a database of 27 million records of derogatory information used by consular officials to screen visa applicants for travel to the United States.[105] On this occasion, Abdulmutallab's name was spelled correctly. The CLASS entry, which matches derogatory information to current visa holders in the CCD, resulted in a "lookout" that connected Abdulmutallab's status as a visa holder with the information provided by his father. By design, the CLASS system only transmitted this information to the primary lookout system used by DHS. This information was merely "accessible" to two agencies primarily responsible for managing air travel watchlists, the Federal Bureau of Investigation's Transportation Screening Center (TSC) and NCTC, but was not required reading.[106]

However, it is doubtful whether the misspelling in the initial Visa Viper cable contributed to the overall "failure" to detect the AQAP plot. The correctly spelled, more detailed cable and the CLASS entry revealing Abdulmutallab's visa status were eventually consolidated into a single file. Depending on the timeframe in which this consolidation occurred, it is not

[98] *Id.*
[99] *9/11 Commission Report* at 400, *supra* note 38.
[100] PNSR REPORT at 113, *supra* note 64.
[101] Wassem, *Immigration: Terrorist Grounds for Exclusion*, at 20, *supra* note 13.
[102] *Intelligence Reform, Part I Before the S. Comm. on Homeland Security and Governmental Affairs*, *supra* note 12 (testimony by Patrick Kennedy, Under Secretary for Management, U.S. Department of State).
[103] Wassem, *Immigration: Terrorist Grounds for Exclusion*, at 20, *supra* note 13.
[104] *Securing America's Safety: Improving the Effectiveness of Anti-Terrorism Tools and Inter-Agency Communication Before the S. Comm. on the Judiciary*, 111th Cong. (Jan. 20, 2010) (statement by Patrick Kennedy, Under Secretary for Management, U.S. Department of State).
[105] *Sharing and Analyzing Information to Prevent Terrorism Before the H. Comm. on the Judiciary*, *supra* note 35 (statement by Patrick Kennedy, Under Secretary of State for Management, Department of State).
[106] *Id.* The Terrorist Screening Center, managed by the FBI was established pursuant to Homeland Security Presidential Directive 6, signed by President Bush in 2003.

unreasonable to assume the validity of State's assertion that "…the misspelling – our error – was obviated" by the pairing up of the correctly spelled cable and the CLASS entry providing visa information on Abdulmutallab."[107]

B. The Decision Not to Revoke Abdulmutallab's Visa[108]

In congressional hearings following the Christmas Day attack, State officials repeatedly pointed out that TSC is responsible for the continual vetting of names located in TSC's Terrorist Screening Database (TSDB) and maintaining the secondary screening ("Selectee") and "No Fly" watchlists. To determine whether individuals in the TSDB hold visas, all records added to the TSDB are checked against the State's CCD.[109] When a match occurs, TSC sends a notice to State to flag cases for visa revocation and, according to a State official, "In almost all such cases, visas are revoked."[110] Notices can also be sent from NCTC and DHS.

Alhaji Umaru's visit to the Embassy in Abuja and the subsequent discovery of Abdulmutallab's status as a visa holder would seem alarming to any reasonable observer. Even assuming State and DHS were the only departments fully aware of the situation by November 20 (as NCTC had received the Visas Viper cable without information regarding Abdulmutallab's visa status), and further assuming that these two pieces of information were all that was known to either department, revocation of Abdulmutallab's visa should have at least been considered. Congressional hearings shed light on why Abdulmutallab was permitted to retain his visa after November 20.

One explanation is that the meetings on November 19 and 20 simply did not provide sufficient information to justify visa revocation.[111] As noted earlier, NCTC placed Abdulmutallab's name on the TIDE list upon receiving the cable from the Abuja Embassy. Pursuant to established protocol, once Abdulmutallab was added to TIDE, an NCTC analyst had to determine whether there was a "reasonable suspicion" that Abdulmutallab intended to engage in a terrorist attack.[112] Had the "reasonable suspicion" standard been met, Abdulmutallab would have been nominated for inclusion on TSC's TSDB and possibly considered for placement on the Selectee or No-Fly lists. Based on State's initial report to NCTC, which contained scant details and made no mention of Abdulmutallab's status as a visa holder, NCTC was justified in not sending his name to TSC. Although NCTC plays an advisory role in the visa revocation process, revocation "would have only occurred if there had been a successful integration of intelligence" by NCTC.[113] It would be tempting to conclude that NCTC's failure to connect the dots, then, played a role in the decision not to revoke Abdulmutallab's visa. Even if this were the case, it is far from clear that NCTC should be held to account – NCTC analysts had relatively little cause to strictly scrutinize the Visa Viper cable, as the State officials who drafted it did not include any assessment of its significance and offered no recommendations as to how NCTC should regard the information.

Although consular officers and the Secretary of State have discretionary authority to revoke a visa at any time,[114] and consular officers are able to revoke visas on terrorist grounds, it is common practice for State to defer to NCTC to identify suspected terrorists and make the proper designations prior to visa revocation.[115] State officials have confirmed that, in accordance with established protocol, both the November 20 Visa Viper and the amended version, sent on November 25, went to proper IC and law enforcement offices to solicit additional information on Abdulmutallab.[116] While NCTC plays an integral part in the advisory process that decides whether visas should be revoked, it does not, contrary to an implication made by a State official testifying before Congress, have authority to unilaterally revoke visas. This official's implication drew a harsh rebuke from Senator Collins and prompted NCTC Director Leiter to jokingly express his surprise at learning of NCTC's newfound visa revocation authority.[117]

State officials also drew the ire of Congress by repeatedly noting that DHS also possesses a measure of authority over visa revocation.[118] Although State did not explicitly suggest that DHS should have assumed

---

[107] *Securing America's Safety: Improving the Effectiveness of Anti-Terrorism Tools and Inter-Agency Communication Before the S. Comm. on the Judiciary*, *supra* note 104.

[108] Although the legislative ambiguity underlying the CT community is amply demonstrated by both the decision-making process with respect to visa revocation and the failure to nominate Abdulmutallab to either the "selectee" or "no fly" watchlists, the explanations for non-revocation and the failure to watchlist dovetail. A discussion of watchlisting practices and how they applied to Abdulmutallab is omitted.

[109] *Sharing and Analyzing Information to Prevent Terrorism, H. Comm. on the Judiciary*, *supra* note 35 (statement of Patrick Kennedy).

[110] *Id.*

[111] Wassem, *Immigration: Terrorist Grounds for Exclusion*, at 20, *supra* note 13.

[112] Laura Rozen, *What Happened After NCTC Got Report on Abdulmutallab*, POLITICO, Dec. 29, 2009.

[113] *White House Review*, *supra* note 3.

[114] Immigration and Nationality Act, Section 221(i); codified at 8 USC § 1201(i).

[115] Wassem, *Immigration: Terrorist Grounds for Exclusion*, at 20, *supra* note 13.

[116] *Flight 253: Learning Lessons from an Averted Tragedy Before the H. Comm. on Homeland Security*, 111th Cong. (Jan. 27, 2010) (statement of Tim Kennedy, U.S. Department of State).

[117] *Lessons and Implications, Part I Before the S. Homeland Security Comm., supra* note 36. Sen. Collins took State to task, stating "At the very least, [Abdulmutallab] should have been required to report to our embassy and explain his activities and answer questions before he was allowed to retain his visa. [State] has this authority…But [State] failed to act. Most disturbing, [State] is also pointing fingers at other agencies to explain this failure." Leiter jokingly responded that he was surprised to learn from the State Department that NCTC had visa revocation authority. *Id.*

[118] *Flight 253: Learning Lessons from an Averted Tragedy Before the H. Comm. on Homeland Security*, *supra* note 116 (statement of Tim Kennedy, "[t]he Department has a close and productive partnership with DHS, which has authority for visa policy"); *see also* Wassem, *Immigration: Terrorist Grounds for Exclusion*, *supra* note 13, for a full discussion of State and DHS's respective authorities over visa issuance and revocation.

responsibility for revocation, the question of DHS's role in visa revocation and, more generally, its existential purpose as a member of the IC muddied the waters enough for congressional members to take aim at DHS despite its utter lack of involvement in any decision regarding Abdulmutallab prior to Christmas Day. DHS Secretary Janet Napolitano felt compelled to spell out, in simple terms, DHS's basic role in both the IC and the immigration process:

> What is our contribution in the INA [immigration/visa policy] field? And the fundamental contribution…is to take information, intel that has been gathered and analyzed, and to push that out -- push that out operationally where it needs to go, or push that out, most importantly -- or as importantly -- to state and local law enforcement.[119]

Other statements by DHS officials have reinforced the notion that it views its primary role in the intelligence process with respect to immigration information is that of consumer, rather than producer.[120]

Despite the uncertainties in roles and responsibilities among State, DHS, and NCTC revealed by congressional inquiry regarding the visa revocation process, it is unlikely that this confusion played a major role in the decision not to revoke Abdulmutallab's visa. There is, in fact, a far more compelling explanation.

C. Going Commando: The Central Intelligence Agency and The Explanation Underneath it All

The driving force behind the decision not to revoke Abdulmutallab's visa can be inferred from a common refrain of State officials during congressional testimony: "There have been numerous cases where our unilateral and uncoordinated revocation would have disrupted important investigations that were underway by one of our national security partners."[121] Federal regulations sanction this practice: the Foreign Affairs Manual instructs consular officers, when they suspect a visa revocation may involve law enforcement interests, to consult with other agencies to determine whether revocation would hinder a law enforcement or intelligence investigation.[122] Reports indicating that Abdulmutallab's father met with CIA officers during his visit to the Embassy in Abuja suggest CIA had a part to play in the decision not to revoke the visa.

CIA, whose absence in the public records detailing the events leading up to the Christmas Day attack is both conspicuous and understandable, undoubtedly viewed the information gleaned from the Abuja meetings as an opportunity. Rather than merely preventing one extremist from boarding a U.S.-bound flight, CIA would use the information gathered on Abdulmutallab to locate and identify the more dangerous threat posed by his sponsoring network. While tracing CIA's involvement with the investigation of Abdulmutallab is an assumptive exercise given the covert nature of CIA operations, there can be little doubt that CIA counseled against visa revocation so as not to spook Abdulmutallab and maintain the operational flexibility necessary to eventually roll up the AQAP network.[123]

CIA's involvement with the case of Abdulmutallab, however, extends beyond its role in counseling against visa revocation. Intelligence officers in the Abuja Embassy notified CIA headquarters of the meeting with Abdulmutallab's father. Media accounts suggest CIA analysts immediately compiled biographical information on Abdulmutallab.[124] However, due to an "oversight mistake of an individual office" within CIA, the information "was not disseminated in a way that it was widely available to the rest of the intelligence community."[125]

While this failure to share information might evoke the information hoarding among the IC that, the 9/11 Commission concluded, permitted the 9/11 plotters to carry their plan through to completion, NCTC Director Leiter insisted that this mistake was "still different from what happened on 9/11."[126] Leiter did not publicly attribute much significance to the oversight and, in fact, lauded State and CIA for convening after the meeting with Alhaji Umaru and deciding to make a recommendation to NCTC to nominate Abdulmutallab for inclusion on TIDE.

D. Lessons From Abuja: The Naked Truth

The handling of information obtained from the November 19 and 20 meetings, the decision not to revoke Abdulmutallab's visa, and whatever responsive (and unknown) action taken as a result of the information should be contextualized with reference to the discussion offered in Part II. The confusion over who, between State and NCTC, bore the burden of flagging Abdulmutallab as a threat worthy of consideration for inclusion on the Selectee or No Fly watchlists was never resolved because State deferred to CIA's judgment in how to address the information provided by Alhaji Umaru. Neither State nor NCTC felt they needed to take the initiative on flagging

---

[119] *Aviation Security and Flight 253 Before the S. Comm. on Commerce, supra* note 22 (testimony of DHS Secretary Janet Napolitano).

[120] *Securing America's Safety: Improving the Effectiveness of Anti-Terrorism Tools and Inter-Agency Communication Before the S. Comm. on the Judiciary supra* note 104, (statement of David Heyman, Assistant Secretary for Policy, Department of Homeland Security).

[121] *Flight 253: Learning Lessons from an Averted Tragedy Before the H. Comm. on Homeland Security*, *supra* note 116. Kennedy explicitly stated that this was the case with Abdulmutallab, *see infra* note 122.

[122] 22 CFR § 41.

[123] Kennedy acknowledged that this was indeed the case with Abdulmutallab, noting, "And one of the members [of the IC] -- and we'd be glad to give you that out of -- in private -- said, "Please, do not revoke this visa. We have eyes on this person. We are following this person who has the visa for the purpose of trying to roll up an entire network, not just stop one person," *supra,* note 116.

[124] *Early Leads Before the Attack*, *supra* note 11.

[125] *Aviation Security and Flight 253 Before the S. Comm. on Commerce, supra* note 22 (testimony of Michael Leiter, Director, NCTC).

[126] *Id.*

Abdulmutallab; CIA was on the case. Although any clandestine operations conducted against Abdulmutallab and AQAP as a result of the meetings are classified, it is a safe assumption that DSOP's role in operational planning was negligible. As discussed in Part II, CIA's primacy in conducting CT operations, taken together with the fact that it did not share its biographical profile of Abdulmutallab with NCTC, suggest that any action taken subsequent to the Abuja meetings did not involve much consultation with NCTC despite its nominative role as the CT community's central hub.

Given the difficulty in discerning the particulars of CIA action taken as a result of the Abuja meeting, it cannot be categorically concluded that this episode is illustrative of the problems identified in Part II. However, the fact that both State and NCTC were justified in not assuming responsibility for taking further action on visa revocation is telling. NCTC did not follow up on the information for any or all of several reasons: it did not have the resources to do so and was therefore unable to correlate the information collected at Abuja with other available "dots"; State either did not realize or did not properly emphasize the gravity of the threat in the Visa Viper cable; and/or CIA had assumed responsibility for formulating and conducting an operational response as a result of the information obtained from Alhaji Umaru. State was similarly blameless, as it rightly deferred to NCTC to search for further information on Abdulmutallab – which did not request any further information from State – and it deferred to CIA to formulate operational follow-up. Assuming CIA formulated a plan without consulting NCTC regarding its implementation, it too should not be held to account. Its actions accorded with its historical autonomy and purpose, and there is no statutory provision requiring it to defer to NCTC's judgment in operational planning. The conclusions and recommendations in Parts V and VI, respectively, do not to suggest that NCTC should be dictating how CIA carries out CT operations. The discussion above is offered to highlight that DSOP is incapable of ensuring that it even be made aware of CIA activity so that it can, at the very least, adjust its planning process to account for ongoing operations. It is also offered to raise a more fundamental question: if, as suggested above, State, NCTC, and CIA performed largely in accordance with their design, how did the CT community "fail" to stop Abdulmutallab from boarding Flight 253?

Proponents of maintaining the statutory status quo of the CT community may argue that the connection between the legislative underpinnings of the CT community and the handling of the information provided by Alhaji Umaru at Abuja is tenuous. But this argument does not address a more salient question: what should the appropriate response to the Abuja meetings have been? The answer to that question should entail a consideration of the legislative framework, discussed in Part II, and the function and purpose of NCTC, CIA, and State in the U.S. government's greater CT efforts.

IV. THE BLAME GAME: UNDER WHERE CAN WE HIDE?

It did not take long after the Christmas Day attack for the finger-pointing to begin in earnest. Many blamed NCTC for failing to piece together information.[127] NCTC Director Leiter was lambasted for going on vacation immediately following the attack.[128] Others held CIA responsible for not having shared biographical data on Abdulmutallab with other agencies.[129] State was roundly criticized for "failing to act" to revoke Abdulmutallab's visa following his father's visit to the Abuja consulate.[130] DHS Secretary Napolitano was taken to task in absentia by a congressional member for not attending a congressional hearing.[131] The former vice president, Dick Cheney, launched withering attacks on President Obama for demonstrating weakness in the War on Terror.[132] Administration officials shot back, blaming the previous administration for allowing al Qaeda to regroup by shifting its focus to military operations in Iraq.[133] It did not take long for administration officials to start taking aim at one another.[134]

Eager to assign blame,[135] many congressional members demanded to know why no one had been fired as a result of the attack.[136] Either the desire to score

---

[127] *Spy Agencies Failed to Collate Clues on Terror*, *supra* note 29.
[128] *White House Defense Terror Aide's Vacation Day After Dec. 25 Attack,* NEW YORK POST, Jan. 7, 2010.
[129] *Spy Agencies Failed to Collate Clues on Terror*, *supra* note 29.
[130] "At the very least, he should have been required to report to our embassy and explain his activities and answer questions before he was allowed to retain his visa. The State Department has this authority…But the State Department failed to act. Most disturbing, the State Department is also pointing fingers at other agencies to explain this failure." *Lessons and Implications, Part I Before the S. Homeland Security Comm, supra* note 36 (remarks by Sen. Susan Collins). NCTC Director Leiter jokingly responded that he was surprised to learn from the State Department that NCTC had visa revocation authority. *Id.*
[131] Rep. Paul Broun stated he was "incensed" that Secretary Napolitano was not in attendance (she was in Spain during the hearing, negotiating for stricter passenger screening standards in foreign airports). *Flight 253: Learning Lessons from an Averted Tragedy Before the H. Comm. on Homeland Security*, *supra* note 116.
[132] *Spy Agencies Failed to Collate Clues on Terror*, *supra* note 29.
[133] *Id.*
[134] Although Leiter largely accepted responsibility, he offered some criticism of other offices, stating "I was surprised at the extent to which other agency searches weren't hitting against very critical data sets that might've uncovered this and then highlighted them for NCTC…" *Lessons and Implications, Part I Before the S. Homeland Security Comm.*, *supra* note 36. FBI Director Mueller, when asked during congressional testimony which agency is responsible for conducting follow-up investigations on threat streams, seemed to point the finger at CIA in stating that "some person" should have, and did not, pass information to NCTC prior to the attack.
[135] Sen. Dorgan stated, "This is a tough job. But still, I -- I think you and us need to understand what failed, and who failed and who's accountable." *Aviation Security and Flight 253 Before the S. Comm. on Commerce, supra* note 22.
[136] *Flight 253: Learning Lessons from an Averted Tragedy Before the H. Comm. on Homeland Security*, *supra* note 116 (Rep. Broun declared, "I think the president of the United States should ask for the -- the resignation of Secretary Napolitano and get somebody there who is not in la-la land"). Sen. McCain, in a separate hearing, inquired of administration officials as to

political points or a fundamental lack of understanding of the CT community's function and capabilities prevented many in Congress from parsing through the complexity of events leading up to the Christmas Day attack to determine what went wrong. In response to Congress's barrage of accusatory questioning, CT officials offered assurances that the system is sound and needs only minor modification. Any additional authorities required by the DNI and/or NCTC will be minor.[137] Rest assured, remedial measures are being taken, improvements are being made, responsibilities are being straightened out,[138] and a comprehensive interagency process is taking place to ensure that this does not happen again. Surely, a person who leaves a trail identical to that of Abdulmutallab will not have the opportunity to board a U.S.-bound flight.[139]

Much of the dialogue in congressional hearings was tragically misguided. Aside from simple human error and failure to follow protocol as described in Part III, neither of which were determinative factors in the ultimate outcome, it is not clear that any "failure" actually occurred. Even with respect to NCTC's "failure" to connect the dots, Leiter's comments on the matter are particularly noteworthy:

> The…category of -- of failing is did you connect these two pieces of data? I frankly think that [this] category is a lot harder to identify and -- and clearly say you made a mistake. We want analysts to do that. But whether or not they actually could, and piece that all together, given the resources, the workload they are facing, it's -- I think it's much more difficult to say that that was a clear failure.[140]

While many congressional members were content to chalk the near success of the AQAP plot up to a failure by the CT community, Leiter's testimony, perhaps unintentionally, seemed to implicitly implore Congress to conduct a more thorough examination of the adequacy of the current structure of the CT community. That the AQAP plot was not detected can only be regarded as a "failure" insofar as the CT community did not perform as Congress hoped it would. In reality, Congress had stacked the deck against CT efforts through deficient legislation and the CT community performed according to its design. If the deck is to be reshuffled to ensure a higher probability of success in CT efforts, Congress will have to play a critical role. As much of the information regarding terrorist threats and CT operations remains classified, congressional understanding of the CT community is particularly important.[141] As the PNSR found, congressional support and oversight of NCTC is complicated by the fact that Congress does not fully understand NCTC's function or value.[142] Throughout congressional hearings committee members repeatedly expressed confusion regarding what NCTC does or is capable of doing.[143]

That is not to say that the cause for further reform is lost, however. During the hearings, certain lines of questioning homed in on the confusion in authority between NCTC and the rest of the IC,[144] revealing an acknowledgment by several congressional members of a central problem, legislative ambiguity, affecting CT efforts.[145] A hearing before the Senate Committee on Homeland Security and Governmental Affairs got to the

---

whether they had fired any personnel as a result of the attack). *Lessons and Implications, Part I Before the S. Homeland Security Comm.*, *supra* note 36.

[137] *Lessons and Implications, Part I Before the S. Homeland Security Comm.*, *supra* note 36 (DNI Blair noted "[t]he authorities of the DNI, I think, heretofore were able to make the big pieces happen. There was lots of -- there was lots of sharing of information in this -- in this case. What we're finding now is some individual pieces in which I think more authority may be required).

[138] Blair: We have a 30-day deadline that the president established to provide authoritative proposed pieces of paper that could be anything from executive order down to an intelligence community directive that -- which I would sign or -- or similar authorities within Secretary Napolitano's organization.

[139] *Current and Projected Threats to the U.S. Before the S. Select Comm. on Intelligence*, 111th Cong. (Feb. 2, 2010) (DNI Dennis Blair confidently asserted that, "I'm confident that someone who left the trail that Mr. Abdulmutallab did would now be -- would now be found").

[140] *Flight 253: Learning Lessons from an Averted Tragedy Before the H. Comm. on Homeland Security*, *supra* note 116 (statement by Michael Leiter, Director of NCTC).

[141] Gov. Thomas Kean testified, "[s]o the public cannot really get involved because of the nature of the information. So we are dependent in this area, more than any other, on congressional oversight. And that's why we made such a point in our report of saying how important we thought congressional oversight was." *Intelligence Reform: The Lessons and Implications of the Christmas Day Attack, Part II Before the S. Comm. on Homeland Security and Governmental Affairs*, *supra* note 44.

[142] PNSR REPORT at XV, *supra* note 64.

[143] *Securing America's Safety: Improving the Effectiveness of Anti-Terrorism Tools and Inter-Agency Communication Before the S. Comm. on the Judiciary*, *supra* note 104 (Senator Whitehouse expressed confusion regarding NCTC capabilities, stating "And I don't know that our NCTC system is designed to play in that quick a timeline or even to search for passenger characteristics that would seem to be inconsistent with the nature of the -- of the flight").

[144] Rep. Pascrell's statement with respect to the State Department's misspelling of Abdulmutallab's name was particularly astute: This is human error, but maybe it's human error precipitated by the fact that we have created a bureaucratic nightmare so that no one is held accountable. *Flight 253: Learning Lessons from an Averted Tragedy Before the H. Comm. on Homeland Security*, *supra* note 116.

[145] *The Lessons and Implications of the Christmas Day Attack: Intelligence Reform and Interagency Integration Before the S. Comm. on Homeland Security and Governmental Affairs*, *supra* note 71. Senators Lieberman and Collins are acutely aware of the legislative deficiencies afflicting NCTC. Senator Collins' opening statement in a March 17 hearing raised several salient points:

> The question is, however, whether or not these authorities have been used as often, as effectively, and in the manner that Congress intended. For example, does the institutional resistance of agencies like the CIA make the use of these authorities such an onerous ordeal that the…DNI is hesitant to embark upon the journey? Is the DNI concerned that exercising these authorities more aggressively might create ill will that will make it even more difficult to coordinate activities in other areas?

heart of the matter. A former DNI official's testimony noted many of the successes of intelligence reform and ably attacked many of the common criticisms of the DNI, concluding that executive branch support and guidance is essential to addressing the issues of overlapping and otherwise unclear lines of authority.[146] A former CIA official put the onus elsewhere. The official's frank assessment was that "Congress gave the DNI broad responsibility, but not clear authority to carry out many of these responsibilities," and this confusion "lies at the heart of the problem."[147] CIA's institutional resentment towards the DNI is well-documented and stems from a number of perceived affronts, not least of which is the DNI's nominative primacy in the IC, but the official's testimony offers clear evidence that "friction" and "mistrust" among the IC primarily results from confusion over authority and function. All sides of the debate seem to agree that the allocation of authorities and responsibilities of the DNI and NCTC should be clarified by, at the very least, the president. The CIA official went a step further, challenging Congress to "take a fresh look at th[e] statute."[148]

V. Conclusion: Always Be Prepared, *Semper Ubi Sub Ubi*

The complexity of the system we have in place today to ensure the nation's security from terrorism can be overwhelming. The system reflects the broad diversity of major players, dozens of strategic objectives, and an intricate web of relationships, roles, and responsibilities. It evolved largely in a piecemeal, ad hoc fashion, without the benefit of an overarching strategy or blueprint for how best to organize for success. In part, the complexity of the current system is due to successive administrations redefining relationships, roles, and responsibilities often without rescinding or fully integrating with the direction established by their predecessors.[149]

The "systemic breakdowns" and "human errors" identified by the White House Review only partially account for the inability of the CT community to identify and disrupt the Christmas Day attack. Despite inconsequential human errors and failure to follow protocol the system, as DHS Secretary Napolitano was criticized for saying, "worked."[150] Any "failure" should be regarded as a natural consequence of an inadequate legislative framework underlying the CT community. This framework gives rise to a disunity of effort that bears far more resemblance to the disjointed and divergent efforts of the IC and law enforcement agencies prior to the attacks on 9/11 than either the administration or Congress care to admit. The non-disruptive improvements being made by DHS, State, NCTC, and FBI are consistent with the overall development of the CT community—they are piecemeal, ad hoc responses to the most recent threatening event.

The most difficult challenge facing the CT community is "deciding what's a threat in the first instance."[151] This task often falls to NCTC and CIA. Information sharing and analysis are the key ingredients to identifying these threats. Information sharing has improved since IRTPA, but problems remain. Some of those problems were made clear by the events leading up to Christmas Day, but they were relatively minor in scale and it is doubtful they contributed in any significant measure to the inability to detect the AQAP plot.

Information analysis is the primary means to identify threats. Given the incredibly high traffic of intelligence received by the IC, technological limitations that hinder the ability to sift through the data, and insufficient manpower to manage the data, connecting fragmentary "dots" will remain a primary challenge. Technological improvements are being made, but they will do little if NCTC is unable to hire more analysts, receive raw data and finished intelligence products from those components in a timely manner, and solicit follow-up assistance from the rest of the IC.

When threats are identified, follow up investigation must run those threats to the ground. NCTC claims to be expanding the scope of threat streams that receive further investigation and tasking "pursuit teams" with this specific purpose.[152] These narrowly-focused teams, however, are analytic units only. As described by one media report, the new pursuit teams "will be responsible for identifying threads of information — the warning Mr. Abdulmutallab's father gave to officials at the United States Embassy in Nigeria, for instance — and tracking and connecting them to other tips."[153] While the development of pursuit teams is an obvious step in the right direction, it is only a first step. Responding to the intelligence is the other part of the equation, and inadequate interagency cooperation and disunity of effort, identified by the 9/11 Commission as fatal flaws in the CT system that prevented detection and interdiction of al Qaeda cell members who carried out the 9/11 attacks,[154] continue to plague the CT community.

Intelligence experts categorically advocate for more senior-level support and involvement, particularly from the President, in clarifying the lines of authority within the IC.[155] The President has taken a number of

---

[146] *Id.* Testimony of the Hon. Benjamin Powell, Former General Counsel to the office of the DNI.
[147] *Id.* Testimony of the Hon. Jeffrey H. Smith, former General Counsel to CIA.
[148] *Id.*
[149] PNSR Report at 1, *supra* note 64.
[150] Peter Baker and Scott Shane, *Obama Seeks to Reassure U.S. After Bombing Attempt*, N.Y. Times, Dec. 28, 2009, appearing at A1.
[151] *Lessons and Implications, Part I Before the S. Homeland Security Comm.*, *supra* note 36 (testimony of Michael Leiter, Director of NCTC).
[152] *Id.*
[153] Eric Schmitt, *New Teams Connect Dots on Terror Plots*, N.Y. Times, Jan. 29, 2010, appearing on A3.
[154] *9/11 Commission Report*, at 401, *supra* note 38.
[155] *The Lessons and Implications of the Christmas Day Attack: Intelligence Reform and Interagency Integration Before the S. Comm. on Homeland Security and Governmental Affairs*, *supra* note 71 (testimony of Benjamin Powell, Former General Counsel to DNI); *also* Gov. Thomas Kean goes so far as to say it is the sole responsibility of the President to clear up authority and budgetary issues: "These ambiguities can cause mission confusion and sometimes a lack of clarity, perhaps, in the lanes in the road. But the burden is on the president to be clear on who is in charge of the intelligence community and where final

steps towards accomplishing this end. Following the Christmas Day attack, he directed NCTC to design a process "whereby there would be follow-up of priority threat streams." Leiter believes this "will be an empowering of strategic operational planning" that will allow NCTC "to demand accountability at a more tactical level for more and a broader range of threats."[156] Intelligence officials by and large seem content that executive branch guidance will address the confusion of authority, and they largely deny that any substantive statutory amendment needs to occur to address the flaws revealed by the Christmas Day attack. It is also worth considering that the Christmas Day attack might have provided the impetus for CT offices to submit to NCTC's interagency processes.

However, there is only so much clarity that executive orders can provide amidst a background of legislative ambiguity. After all, §1018 called for this exact guidance in 2004 by instructing the president to "issue guidelines to ensure the effective implementation and execution…of the authorities granted to the DNI,"[157] and this guidance, in the form of an amended EO 12,333, has brought the IC to its current state.[158] As long as the underlying statutory regime limits NCTC's ability to solicit meaningful interagency cooperation while insisting NCTC serve as the "central hub" of all CT efforts, improvement in CT coordination is likely to be short-lived.

authority lies on budget and on personnel matters." Lee Hamilton agrees with this assessment. *Intelligence Reform: The Lessons and Implications of the Christmas Day Attack, Part II Before the S. Comm. on Homeland Security and Governmental Affairs*, *supra* note 44.

[156] *Lessons and Implications, Part I Before the S. Homeland Security Comm.*, *supra* note 36 (testimony of Michael Leiter, Director of NCTC).

[157] IRTPA, P.L. 108-458.

[158] *Lessons and Implications, Part I Before the S. Homeland Security Comm.*, *supra* note 36. DNI Dennis Blair's remarks at a recent congressional hearing provide a frank assessment of the current state of the CT community:

> I think you're putting your finger…on a characteristic of the -- this combating terrorism effort that we need to tighten down with the -- with the strong enthusiasm for counterterrorism, the -- a sense that we all have to be working on it. I think we did not drive some of these responsibilities as far as we should of in terms of, "No kidding. OK, everybody's -- everybody's helping, but who is it -- who is it at the end?" And I think…we need to, and are going to tighten right down so that primary responsibilities, support responsibilities and ultimate responsibility are made to -- are – are made clearer. Because there -- there is a tendency to say, "Hey, I've got this new capability. Let me help you." And -- and we ought to do that. But we should not allow that to interfere with a -- with a clear understanding of who -- who has the ultimate call.

VI. Recommendations: Stitching Up the Holes That Leave Us Dangerously Exposed

Intelligence reform is incomplete. Abdulmutallab's ability to slip under the radar resulted from a lack of clear-cut delineation of authority and responsibility among the members of the CT community. It is incumbent upon the President *and* Congress to eliminate the present confusion and complete the reforms of the IC undertaken in response to 9/11. Below are recommendations of measure to achieve this objective.

The conflation of the terms "strategic" and "operational" in the name and mission of the Directorate of Strategic Operational Planning "has hindered DSOP since its inception and remains a significant problem."[159] As noted, "joint," not "strategic," was the descriptor preferred by the 9/11 Commission. The term was opposed by those CT components charged with carrying out operations, which bristled at the possibility of ceding authority to a DNI-based office.[160] The term "strategic," which was meant to emphasize the role of DSOP, and more generally NCTC, as the interlocutor between the NSC and various CT components charged with operations, has put DSOP in a "planning no man's land."[161] One way to address this problem is to bifurcate the DSOP into "strategic" and "tactical" components. However, bifurcation is a minor adjustment and does not address the underlying, more contentious issue of which office properly holds the authority to conduct operations.

A former DSOP official argues that although the authority to execute operations should not be granted to DSOP, it should be given increased authority over its resources and personnel.[162] Increased authority might improve the credibility of the DSOP among members of the IC and increase interagency participation in the planning process. However, this model, like that of the Joint Chiefs of Staff, seems more adequately suited to bolstering strategic planning rather than improving the IC's ability to respond to the exigencies of the day, and does not bring DSOP fully "in the loop" with respect to CT operational planning.

Both the military, on the one hand, and the intelligence and law enforcement communities, on the other, engage in strategic planning. A critical difference between the two is that the CT efforts of intelligence and law enforcement communities are more heavily focused on taking preventive action. For that reason, the Joint Chiefs model is ill-suited for the IC. As there is general agreement that NCTC should not have operational authority, there are two alternative methods of ensuring the IC's responsiveness to NCTC through executive order, both of which require dramatic transformation of

[159] *The Lessons and Implications of the Christmas Day Attack: Intelligence Reform and Interagency Integration Before the S. Comm. on Homeland Security and Governmental Affairs*, *supra* note 71 (testimony of Richard Nelson, former DSOP official).

[160] PNSR Report at 49-51, *supra* note 64.

[161] *The Christmas Day Attack: Intelligence Reform and Interagency Integration Before the S. Comm. on Homeland Security and Governmental Affairs*, *supra* note 71 (testimony of Richard Nelson, former DSOP official).

[162] *Id.*

the IC.

First, all terrorism-focused analytical components of the IC could be placed literally under the roof of NCTC. Folding terrorism analysts into the NCTC's Directorate of Intelligence, with NCTC exerting direct authority over the analysts, presents significant logistical obstacles that were present in the initial establishment of the DNI.[163] However, NCTC's absorption of analysts from the IC at large would force every member of the IC to look to NCTC for strategic and operational guidance, thereby fulfilling the statutory mandate that NCTC serve as the central hub of information sharing. By giving DSOP unfettered access to all terrorist threat-related information and personnel by virtue of its proximity to the strengthened NCTC DI, DSOP would have a better vantage point from which to assign roles and responsibilities in CT operations.

A second, more practicable but perhaps no less transformative option is to fold NCTC into CIA's CTC. The CIA is the "only agency that's still…'central'"[164] in terms of its relationships with other IC components, and it remains the only entity responsible for the production of all-source intelligence and capable of conducting covert operations (aside from DoD). Relocating NCTC would strengthen the vertical coordination of CT efforts from the NSC down to satellite programmers and operations officers in the field. With institutionalized collaboration with NCTC, CTC would have access to all terrorism-related information in NCTC's DI, and DSOP would have proximity to those it charges with carrying out operations. NCTC/CTC would form a symbiotic relationship, with each organization accounting for the weaknesses of the other: NCTC would gain an institutionalized advisory role with respect to operational planning while CTC would benefit from NCTC's statutory role as the central hub of international terrorism-related information. Although one result of the aggregation of NCTC and CTC would undercut a central purpose of the 2004 reforms by returning CIA to preeminence among the IC at the cost of further diminution of the DNI's authority, clear statutory language establishing the DNI's superior role and granting additional budget and personnel authority to the DNI would ensure that NCTC and CTC remain subject to DNI authority.

These reforms can be effectuated by executive order without running afoul of existing statutes. The President has broad authority to institutionalize cooperation and coordination of CT activities through NCTC, but Congress also has a part to play. For the reasons mentioned above, Congress should leave the provision denying the NCTC Director the authority to execute operations in place.[165] However, Congress should amend 50 USC § 404o(d)(2) to conform to the recommendations of the 9/11 Commission and give DSOP a part to play in operational planning.

With respect to the primary missions of the NCTC, the amended statute could read as follows: "To conduct *joint* strategic operational planning for counterterrorism activities" [amendment highlighted]. The change is ostensibly minor, but consequential in effect. DSOP would be given a firmer statutory basis for involvement in interagency planning processes. The amendment also preserves the "strategic" function of DSOP, as many IC officials have acknowledged that strategic planning remains a glaring weakness of the IC. Furthermore, NCTC has proven capable of defining the "strategic operational" paradox, presenting another justification for maintaining its "strategic" aspect.

The second statutory amendment required to strengthen DSOP and eliminate confusion will likely be far more politically challenging to codify.[166] Section 404o(j)(2) of 50 USC, pertaining to the DSOP, currently reads (taking conforming changes from the earlier suggested amendment into account):

> (2)*(a) Joint* strategic operational planning shall include the mission, objectives to be achieved, tasks to be performed, interagency coordination of operational activities, and the assignment of roles and responsibilities [amendment emphasized].

To ensure compliance with DSOP functions, Congress could amend current law by adding § 404o(j)(2)(b), which would state:

> (b) Those agencies identified by DSOP as necessary for the performance of missions under (2)(a) shall comply with the tasks assigned them by DSOP pursuant to (2)(a) unless they can show cause that compliance unduly burdens agency resources or requires the agency to perform tasks contrary to those permitted by statute.

With this language, NCTC will be given a place at the table in joint strategic operational planning without running afoul of the prohibition against NCTC's conducting operations. It will allow NCTC to function in accordance with the recommendations of the 9/11 Commission and will permit DSOP to fulfill its statutory obligations.

Congress's attempts to hold someone, anyone accountable for the Christmas Day attack were not guided solely by the need to score political points. Ensuring accountability is indeed a raison d'etre of congressional committees. However, the critical point here is that given diffuse, conflicting, and overlapping authorities and responsibilities among members of the CT community, there is no adequate means of determining accountability. Presidents, current and former, can be blamed for providing insufficient

---

[163] *See generally* Patrick Neary, *Intelligence Reform, 2001-2009: Requiescat in Pace?* STUDIES IN INTELLIGENCE Vol. 54, No. 1 (Extracts, March 2010) (describing the logistical difficulties, compounded by the IC's reluctance to support the DNI, in establishing even a physical presence for the DNI).

[164] *The Lessons and Implications of the Christmas Day Attack: Intelligence Reform and Interagency Integration Before the S. Comm. on Homeland Security and Governmental Affairs*, *supra* note 71 (testimony of the Hon. Jeffrey H. Smith, former General Counsel to CIA).

[165] 50 USC § 404o(g).

[166] As the Hon. Lee Hamilton testified, "that statute was very hard to pass. And it is not going to be amended quickly or soon, so you're going to be living with it." *Aviation Security and Flight 253 Before the S. Comm. on Commerce*, *supra* note 22.

guidance pursuant to § 1018 of IRTPA. However, Congress should recognize itself as responsible in the first instance for establishing a CT community of such complexity as to give rise to the conditions that allowed Abdulmutallab to come so close to bringing down Flight 253. By clarifying roles and responsibilities within the CT community and offering necessary support to certain CT entities to enable them to fulfill their statutory mission, Congress would improve its ability to ensure accountability in the conduct of CT operations.

As the PNSR found, "barring the idea of vesting one individual with directive authority over departments and agencies…there is no silver bullet—no single recommendation that ensures an integrated and unified counterterrorism mission."[167] Several steps need to be taken to strengthen the CT community, and Congress and the President bear the burden. Intelligence reform, begun in 2004, is not yet finished. The "failure" to connect the dots relating to Abdulmutallab has been repeatedly described as a failure to walk "the last tactical mile." It is time to walk the last tactical mile. Abdulmutallab should have never been allowed to board a U.S.-bound flight and, but for perhaps a deficient explosive device, its operator's inability to use it, and the courage and quick thinking of Flight 253's passengers and crew, AQAP would have carried out the most significant terrorist attack against the U.S. since 9/11. Congress and the President have a limited opportunity to right the ship and complete the implementation of reforms recommended by the 9/11 Commission.

VII. A Brief Epilogue

Less than a month following the completion of this analysis, the Senate Select Committee on Intelligence (SSCI) made public portions of a 55-page classified report entitled, *Attempted Terrorist Attack on Northwest Airlines Flight 253*.[168] The unclassified version of the report contained only an Executive Summary and comments. Fortunately, SSCI's primary findings were included in the summary:

- "NCTC was not organized adequately to fulfill its missions"
- No single agency considered itself responsible for "tracking and identifying all terrorism threats"
- Technology across the IC was inadequate to providing analysts with search enhancing tools needed to identify Abdulmutallab[169]

SSCI also identified fourteen specific "points of failure," including "a series of human errors, technical problems, systemic obstacles, analytical misjudgments, and competing priorities" that contributed to the failure to identify Abdulmutallab prior to his boarding Flight 253.[170] The points of failure listed by SSCI were distributed among several agencies, and included: State's failure to revoke Abdulmutallab's visa; the failure to put Abdulmutallab on the TSDB; CIA's failure to search databases containing information relating to Abdulmutallab; the failure to disseminate information to all "appropriate" elements of CIA; CIA's failure to disseminate key reporting until after the attempted attack; CTC's limited name search which failed to produce key information on Abdulmutallab; CTC analysts' failure to connect the dots of information relating to Abdulmutallab; NCTC DI's failure to connect the dots; and NCTC Watchlisting Office's failure to conduct additional research on Abdulmutallab.[171] Most predictably, SSCI faulted IC analysts for "not connecting key reports partly identifying Abdulmutallab," failing to disseminate all available information on Abdulmutallab, and focusing on the threat posed by AQAP to U.S. interests in Yemen rather than to the homeland.[172]

SSCI's recommendations, like its findings, were largely predictable. Regarding visa revocation, SSCI recommended that State exercise "independent judgment and authority" in the revocation process and that NCTC make recommendations to State to "deny or revoke a U.S. visa based on terrorism-related intelligence."[173] On the inadequacy of search-related technology, SSCI charged certain department and agency heads with undertaking a dizzying array of navel-gazing verbs: "review," "report," "develop," etc.[174] In conclusions and recommendations regarding the failure to connect the dots of information on Abdulmutallab, SSCI simply broadened its vocabulary, tasking components of the IC with "ensur[ing] that analysts understand their responsibility," "organiz[ing]" offices in a manner that optimizes analysts' ability to understand available information, and "conducting" additional research on targets.[175] Those following Congress's investigation of the "failures" that allowed Abdulmutallab to board Flight 253 were likely least surprised by SSCI's recommendation that the DNI:

> [R]eview the roles and responsibilities of counterterrorism analysts throughout the [IC] to ensure that all agencies understand their counterterrorism role, their role in identifying and analyzing threats to the U.S. homeland, and that [CT] analysts actively collaborate across the IC to identify

[167] PNSR Report at 13, *supra* note 64.
[168] S. Rep. No. 111-119 (2010).
[169] *Id.* at 1-2.
[170] *Id.* at 2.
[171] *Id.*
[172] *Id.* The report's only revelatory points of failure that had not been previously discussed at length in committee hearings were those of the IC's chief signals intelligence agency, the NSA, which SSCI faulted for not pursuing "potential collection opportunities that could have provided information on Abdulmutallab" and failing to nominate Abdulmutallab for watchlisting based on available information. However, neither the unclassified portion of the report nor committee hearings shed light on which agency, if any, holds responsibility for tasking NSA with collecting additional information. The conclusion cannot be drawn from SSCI's report that NSA itself was responsible for determining that additional collection activities needed to be undertaken to identify Abdulmutallab, particularly since SSCI's qualms with NSA seemed to have more to do with its "backlog of reports that require review for watchlisting" rather than its failure to act on its own initiative to strengthen its collection efforts against AQAP.
[173] *Id.* at 4.
[174] *Id.* at 6.
[175] *Id.* at 6-9.

such threats.[176]

In fairness to SSCI, many of the report's recommendations remained classified. Giving SSCI the benefit of the doubt, it is worth considering that the classified recommendations contained more substance than those included in the Executive Summary. SSCI is to be commended for recognizing that, contrary to assertions by administration officials that the failure to identify Abdulmutallab was unlike those that preceded 9/11 in that it was a failure to understand available intelligence rather than a failure to collect and share information, many of the "failures" that allowed Abdulmutallab to board Flight 253 were, in fact, reminiscent of those identified in the 9/11 Commission Report.

In the end, SSCI's findings were demonstrative of Congress's failure to take responsibility for its own role in the creation of a CT community rife with ambiguity in the roles and responsibilities of its constitutive parts.[177] Perhaps the most telling example of Congress' inability and/or unwillingness to address the uncertainty among the CT community was the fact that the report, while laying blame for the near success of the Christmas Day attack across the CT community, seemed to single out NCTC as the most culpable entity. The report cited the strong language of NCTC's statutory foundation naming it the central hub of all terrorism-related information, concluding "[d]espite its statutory mission, NCTC did not believe it was the sole agency in the IC for piecing together all terrorism threats." The report took NCTC to task for "fail[ing] to organize itself in a manner consistent with Congress's intent or in a manner that would clearly identify the roles and responsibilities necessary to complete its mission"[178] while making no mention of Congress's culpability in undercutting NCTC's ability to fulfill its mission. SSCI's recommendations were a further reflection of Congress' inability to understand its central role in creating and perpetuating the system it so often criticizes.

The unclassified portions of SSCI report validate the central findings of this study. Congress's identification of the various "failures" of the CT community misses the point: the system performed in accordance with its statutory design. Congress's calls for the CT community to "review," "study," "examine," "develop," "ensure," etc. might address the specific "failings" that allowed the Christmas Day attack to occur, but Congress's failure to assertively address the statutory ambiguity underlying the CT community will continue to hinder efforts to combat the threat of terrorism.

[176] *Id.* at 9.

[177] Dr. Amy Zegart has written extensively on intelligence reform and organizational deficiencies among national security agencies. Dr. Zegart has also examined the systemic reasons underlying Congress's inability to understand, much less provide meaningful oversight for, the activities of the IC. Her findings offer considerable context to understanding congressional action taken in response to the Christmas Day attack. *See* Amy Zegart, The Domestic Sources of Irrational Intelligence Oversight, Presentation at the Robert S. Strauss Center for International Security and Law at the University of Texas (Sep. 15, 2010) (summary available at http://www.robertstrausscenter.org/events/125.)

[178] S. REP. NO. 111-119 at 11, *supra* note 168.

Jus Post Bellum: Reflections on the *Right* Way to End a War

Richard M. O'Meara

There can be no Justice in war if there are not, ultimately, responsible men and women.[1]

If you break it you own it.[2]

Peace is not sought in order to provoke war, but war is waged in order to attain peace. Be a peacemaker, then, even by fighting, so that through your victory you might bring those whom you defeat to the advantages of peace.[3]

War is tough stuff. It is, at the very least, the organized projection of death and mayhem by some group against another, generally for purposes of governance.[4] Its justifications are myriad, running the gamut from self-defense, to humanitarian intervention, to national aggrandizement to whim and revenge. And yet, ironically, it is not the most heinous of human activities. As R. J. Rummel has noted in his discussion of *democide*, the murder of civilians by government agents acting authoritatively:

> [I]n total, during the first eighty-eight years of this century [20th century], almost 170 million men, women, and children have been shot, beaten, tortured, knifed, burned, starved, frozen, crushed, or worked to death; buried alive, drowned, hung, bombed, or killed in any other of the myriad ways governments have inflicted death on unarmed, helpless citizens and foreigners. The dead could conceivably be nearly 360 million people. It is as though our species has been devastated by a modern Black Plague. And indeed it has, but a plague of Power, not germs.[5]

Yet, a good deal of Rummel's *democide* has occurred in preparation for war, during war and, indeed, after war has officially ended.[6] Whether one argues that war is *ever* a useful project in the conduct of affairs amongst men, it appears clear that humans have a long history of its use,[7] that it is always terribly destructive,[8] and recourse to arms does not appear to be going away any time soon. The good news is that there is a fairly robust articulation in both law and moral philosophy regarding a political entity's right to start a war-project and how war is to be conducted. On the other hand, these articulations have been confounded by a bewildering set of war paradigms that do not fit neatly into these old articulations. Further, these new types of force projections never seem to end. Finally, it appears clear that failure to end a war well, to win the peace, can

---

[1] Michael Waltzer, *Just and Unjust Wars*, A Moral Argument with Historical Illustrations 4th ed. (Basic Books:New York, 2006), 288.

[2] Secretary of State Colin Powell's advice to President Bush regarding the pending war in Iraq, 2002, referred to generally as the *Pottery Barn Rule*, *as cited by* Bob Woodward, *retrieved at* http://www.buffalo,edu/ubreporter/archives/vol36n13/articles/Woodward.html, 3/5/2010.

[3] St. Augustine, Letter 189, to Boniface, in E.L. Fortin and D. Kries (eds.), *Augustine: Political Writings*, trans. M.W. Tkacz and D. Kries (Indianapolis: Hackett 1994) , 220.

[4] Brian Orend, 'War,' *Stanford Encyclopedia of Philosophy retrieved at* http://plato.stanford.edu/entries/war, 03/26/2010, 1.

[5] R.J. Rummel, *Death by Government* (New Brunswick: Transaction Publishers, 2000), 9.Rummel defines democide as the '..murder of any person or people by a government, including genocide, politicide, and mass murder.' 31. Rummel's statistics are chilling and bear repeating:

> Not even considered thus far is the human cost of war-another way governments act as an agent of death. For the years 1740 to 1897 there were reportedly 230 international and revolutionary wars; according to one count, these wars killed 20,154,000 people. If with more tolerance for gross estimation we accept the calculations that have been made of those killed in all international wars since 30 B.C. we get the 40,457,000 dead shown in table 3.1. This is less than a third of the overall *democide* that we have been able to estimate. There should be little doubt that while pre-twentieth-century war has been of great historical interest and drama, governments have killed many times more people in cold blood than they have in the heat of battle.

Referring to the 20th century, including World Wars 1 and 11, Rummel continues:

> Consider table 1.2 and figure 1.1: the list and its graph of this century's megamurderers-those states killing in cold blood, aside from warfare, 1 million or more men, women and children. These fifteen megamurderers have wiped out over 151 million people, almost four times the almost 38,500,000 battle dead from all this century's international and civil wars up to 1987,. The most absolute Powers-namely, communist USSR, China, and preceding-Mao guerrillas; Khmer Rouge Cambodia, Vietnam, and Yugoslavia, and fascist Nazi Germany-account for nearly 128 million of them, or 84 percent. 3.

[6] Ibid. "I believe that war and *democide* can be understood within a common framework. They are part of the same social process: a balancing of power, where Power is supreme." 22.

[7] See, for example, John Keegan, *A History of Warfare* (New York: Knopf 1993) and Donald Kagan, *On the Origins of War and the Preservations of Peace* (New York: Knopf Doubleday Publishing Group, 1996).

[8] One is reminded of President Eisenhower's warnings regarding preparations for war in 1953:

> Every gun that is made, every warship launched, every rocket fired signifies, in the final sense, a theft from those who hunger and are not fed, those who are cold and are not clothed.
>
> The cost of one modern heavy bomber is this: a modern brick school in more than 30 cities.
> It is two electric power plants, each serving a town of 60,000 population.
>
> It is two fine, fully equipped hospitals. We pay for a single fighter plane with a half million bushels of wheat. We pay for a single destroyer with new homes that could have housed 8,000 people.

Retrieved at http://www.quotedb.com/quotes/405, 03/26/2010.

have catastrophic consequences and lead – even as the dead are buried, the monuments laid and the disabled march home – to future wars.[9] Getting the peace *right*, then, must be considered as important as determining when and how to fight.

What is war?

The use of the term *war* occurs in many contexts and can, even with the best of intentions, lead to very sloppy discussions. At one level, there are the *wars on drugs*, *poverty* and the like which seem to connote an organized and focused effort at the eradication of a particular condition. Somewhere in the middle are a whole host of definitions which come out of domestic law and are meant to trigger certain legal ramifications such as trade restrictions, immigration procedures, emergency powers for governments in the area of civil rights, or rights and responsibilities under insurance contracts. On another level are definitions of war which speak to projections of force by states, each vying with the other in relative symmetry in order to obtain a peace which conforms to the aims and desires of the victor. Finally, there are those asymmetric contests which are fought by states and non-state actors and which arise out of guerrilla wars and insurgencies, wars of intervention, wars against terrorists and terror generally and proxy guerrilla wars.[10]

A standard definition of war, one that carries with it many of the assumptions upon which the UN Charter and subsequent articulations of international law regarding constraints on war generally, appears in L. Oppenheim's treatise on International Law in 1952:

> War is a contention between two or more States through their armed forces, for the purpose of overpowering each other and imposing such conditions of peace as the victor pleases.[11]

Another commentator, Yoram Dinstein, notes that

> In large measure, the classification of a military action as either war or a closed incident ('short of war') depends on the way in which the two antagonists appraise the situation. As long as both parties choose to consider what has transpired as a mere incident, and provided that the incident is rapidly closed, it is hard to gainsay that view. Once, however, one of the parties elects to engage in war, the other side is incapable of preventing that development…
>
> There is a marked difference between war and peace: whereas it requires two States to conclude and to preserve peace…it takes a single State to embroil itself as well as its selected enemy in war.[12]

A third commentator, Christine Gray, eschews the term *war* altogether as she discusses international law (IL) and the *use of force* generally, noting that that is the term which is used by the UN Charter in its prohibition.

> Article 2 The Organization and its Members, in pursuit of the Purposes stated in Article 1, shall act in accordance with the following Principles:
>
> All Members shall refrain in their international relations from the threat or *use of force* against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.[13]

There is a recognition in the 21st century that the classical peace/war dichotomy '…has lost its *raison d'être* with the outlawry of war and the blurring of the boundaries between conflict and peace.'[14] This is especially true in internal armed violence which is reported to form, for example, 95% of all armed violence between 1995 and 2005.[15]

Given that *wars, conflicts, projections of force*, *uses of force* and *activities short of war* all have varying war aims, tend to use multiple methods of conventional and unconventional violence, have different levels of respect

[9] Even a cursory review of the manner in which World War 1 ended, for example, the failure to completely defeat the German army, the terms and conditions of the Treaty of Versailles, the lack of political will by the victors to enforce the terms of the Treaty, must bolster the argument that the peacemakers failed in their task of bringing World War 1 to a successful conclusion. *See generally* Margaret MacMillian, *Paris 1919* (New York: Random House 2003); Manfred F.Boemeke, Gerald D. Feldman, Elisabeth, eds.. *The Treaty of Versailles, A reassessment after 75 Years* (Cambridge: Cambridge University Press, 1998).

[10] Michael L. Gross notes that the dilemmas of asymmetric warfare turn on their head the assumptions and conditions of traditional war between states.

> In each type of conflict, assessments of military necessity, just cause, combatant liability, noncombatant immunity, reciprocity, and concern for future peace will vary. In general asymmetric conflicts differ as a function of the actors involved, participants' goals or war aims, and the means they use to achieve them. Actors range from guerrillas and terrorists on the weaker side to states, coalitions of states, and international forces under UN auspices on the stronger side. Goals range from maintaining the status quo to changing it, and from defeating an enemy decisively in pitched battle to simply staving off defeat in the hopes of setting incontestable conditions for a political settlement…The means of war vary considerably. Some are conventional (missile and artillery) but many other means are unconventional and include torture, assassination, blackmail, terror, and nonlethal weapons.

Michael L. Gross, *Moral Dilemmas of Modern War, Torture, Assassination, and Blackmail in an Age of Asymmetric Conflict* (New York: Cambridge University Press, 2010), 14.

[11] L. Oppenheim, *International Law*, 7th ed .H.Lauterpacht *ed*. (London: Longmans Green & Co., 1952). (1952).

[12] Yoram Dinstein, *War, Aggression and Self-Defense,* 4th ed. (New York: Cambridge University Press, 2005), 11.

[13] Christine Gray, *International Law and the Use of Force,* 2d ed. (Oxford: Oxford University Press, 2004), 3.

[14] Carsten. Stahn, 'Chapter 5 JUS POST BELLUM: MAPPING THE DISCIPLINE(S)' in Carsten Stahn, Jann Kleffner *eds*. *JUS POST BELLUM Towards a Law of Transition from Conflict to Peace* (The Hague: T.M.C. Asser Press 2008), 99.

[15] See Human Security Report 2005, *The Changing face of Global Violence*, 18.

for civilian targets, and are fought by different groups of actors, traditional definitions of war as an activity reserved to states and constrained by state authority would appear to be less and less relevant.[16]

This is not to say, however, that all these categories of violence do not have some things in common. They all, it would appear, comprise elements of violent advocacy; that is, they all use levels of violence to obtain certain goals. While those goals may differ, humanitarian intervention vs. terrorist bomb attacks, violence in one form or another is the primary tool. Further, these activities are carried on by political communities, those who seek to impose their will on other groups through the use of violence. Finally, these activities violate the rights of others for the purpose of changing the way others operate.

Brian Orend melds these different characteristics in his definition of war as follows:

> War should be understood as an *actual*, i*ntentional* and *widespread* armed conflict between political communities…War is a phenomenon which occurs only between political communities, defined as those entities which either are states or intend to become states (in order to allow for civil war). Classical war is international war, a war between different states… [B]ut just as frequent is war within a state between rival groups or communities…Certain political pressure groups, like terrorist organizations, might also be considered 'political communities' in that they are associations of people with a political purpose and, indeed, many of them aspire to statehood or to influence the development of statehood in certain lands.
>
> Indeed, it seems that *all warfare is precisely, and ultimately, about governance.* War is a violent way for determining who gets to say what goes on in a given territory, for example, regarding: who gets power, who gets wealth and resources, whose ideals prevail, who is a member and who is not, which laws get made, what gets taught in schools, where the border rests, how much tax is levied, and so on. War is the ultimate means for deciding these issues if a peaceful process or resolution can't be agreed upon.
>
> War, indeed, is governance by bludgeon.[17]

What is peace?

Peace is not the absence of war. As the discussion above indicates, *war* is a delicate subject susceptible to multiple definitions and interpretations. The construct of *peace* appears to carry with it the same problems. Henry Kissinger, amongst others, cautioned in 1974 that '…two world wars and an era of involvement and conflict should now have taught us that peace is a process, not a condition.'[18] This conclusion has been bolstered in recent years by the considerable violence experienced in Iraq and Afghanistan as well as in multiple peacekeeping operations throughout the world.[19] The cessation of widespread and organized violence, then, does not automatically signal peace and yet its achievement appears to be among humanity's highest values.[20] R.J. Rummel speaks to the fragility of peace:

> …peace is a property of conflict systems and a homeostatic of cybernetic property that enables the system, in the course of its dynamic path, to remain in some stated boundary. Where the boundary is drawn is not so important as the machinery by which the system stays within it wherever it is drawn. Most conflict systems exhibit what might be called a 'Break boundary' at which the system suddenly changes into another or passes some point of no return in its dynamic process. Thus, marital conflict may lead to separation or divorce, industrial conflict may lead to strikes, personal conflicts may lead to fisticuffs at the lower end of the social scale or to litigation at the upper end, and international relations may degenerate into war.[21]

Finally, Rummel notes some of the characteristics of peace:

> ...peace as a social contract is active, not passive. It is created through negotiation, adjustment, resolution, decisions. It comprises predictions (expectations) about the future. It is manifested through cooperative interaction. Its existence depends on congruence with the balance of powers. It is a phase in the dynamics of the conflict helix.

---

[16] Gross, *Moral Dilemmas in Modern War,* 8-25.

[17] Orend, 'War', 1-2.

[18] Henry. Kissinger *as cited in* R.J. Rummel ' Chapter 2 What is Peace?' *in Understanding Conflict and War: v. 5 The Just Peace retrieved* at http://www.hawaii.edu/powerkills/TJP.CHAP2HTM, 03/26/2010.

[19] Serena K. Sharma, 'Chapter 1: RECOSIDERING THE JUS AD BELLUM/JUST IN BELLO DISTINCTION' *in Jus Post Bellum,* 29.

[20] Rummel takes note of this occupation:

> Consider: 'Peace at any price.' 'The most disadvantageous peace is better than the most just war.' 'Peace is more important than all justice.' 'I prefer the most unjust peace to the justest war that was every waged.' 'There never was a good war or a bad peace.' [footnotes omitted].
>
> Yet, we agree little on what is peace. Perhaps the most popular (Western) view is as an absence of dissension, violence, or war, a meaning found in the *New Testament* and possibly an original meaning of the Greek word for peace Irene…Peace, however, is also seen as concord, or harmony and tranquility. It is viewed as peace of mind or serenity, especially in the East. It is defined as a state of law or civil government, a state of justice or goodness, a balance or equilibrium.
>
> Such meanings of peace function at different levels. Peace may be opposed to or an opposite of antagonistic conflict, violence, or war. It may refer to an internal state (of mind or of nations) or to external relations. Or it may be narrow in conception, referring to specific relations in an particular situation (like a peace treaty), or overarching, covering a whole society (as in a world peace). Peace may be a dichotomy (it exists or it does not) or continuous, passive or active, empirical or abstract, descriptive or normative, or positive or negative.

Rummel, *Understanding Conflict and War*, sec 2.1, 1-2.

[21] Ibid, 28.

> By contrast, peace as the absence of violence or war is passive. True, it may be generated by negotiation and resolution. But the resulting peace is inactive, inert. It is a social void-something to build a wall around to protect and maintain. Any condition or structure or lack thereof constitutes such a peace as long as there is no social violence-even a desert without life.[22]

Theorists from Aristotle to Michael Waltzer appear to agree that the aim of war must be peace, albeit a peace defined, at least in part, by the belligerents involved.[23] There is a good deal of literature regarding the rules which might apply to the making of peace and what goals peacemaking should have. These will be discussed below. It should be remembered, however, that most contemporary wars are fought by groups who have previously agreed to terms of peace in one form or another and that the '…average number of conflicts terminated per year in the 1990s was more than twice the average of all previous decades from 1946 onwards.'[24]

What are the rules?

The big questions regarding war and peace have traditionally been articulated as follows:

> When is war justified and who gets to do it? How should we conduct ourselves as we go about the business of war?
>
> How should wars end and what does peace look like?

There are four traditions which dominate the response to these questions: *Just War Theory, International Law*, *Realist Theory*, and *Pacifism*. They all assume that *war*, however it is defined, is a scourge, an activity to be avoided if at all possible. Yet the first three admit to the need to conduct war in various situations and articulate rules for the conduct of war as well.

Just War Theory

Just War Theory is a theory of ethics; it is a review of norms which seeks to determine when the inception of war is *just*, that is morally permitted; what conduct during a war is j*ust*, that is morally acceptable or constrained; and what are the conditions for a just peace, that is what *should* a peace look like. The question here is: what is mankind entitled to do *morally* when it comes to the conduct of war?[25] The history of Just War Theory is long, reaching back as far as Socrates and Aristotle, through Cicero and Augustine, Aquinas, Grotius, Suarez, Vattel and Vitorio to Michael Waltzer, considered the dean of contemporary Just War theorists.[26] Its origins are a synthesis between Greco-Roman and Christian values and as will be seen below, Just War Theory forms the basis for contemporary international law articulations. Its rules, as with much of Western moral philosophy, are found in theology or in the concept of natural law. And it can be said – without too much fear of contradiction and despite the carnage of the last 2500 years – to have influenced the conduct of war profoundly.

Just War Theory speaks to three often considered separate and distinct calculations regarding the conduct of war which answer the questions set out above. To begin a war (jus ad bellum), it must be considered *just*, that is the decision must conclude that there is a *just cause;* there must be a *right intention*; it must be conducted by *proper authorities*; it must be the *last resort*; and there must be a *probability of success*. Finally, and perhaps of considerable import to the question of how to end a war, there must be a determination of *proportionality*, the idea that the universal goods to be obtained outweigh the universal evils which can be foreseen.[27] These determinations are constraints in that they limit the use of war to a very discreet set of situations, such as self-defense, the defense of others, the protection of innocents and punishment of grievous wrong doing; define who can make the determination and who will be in charge of its conduct; and require some consideration of the results of the conduct before war is initiated. Together, these determinations constitute justification for unleashing the projection of force, committing what would otherwise be held to be murder and mayhem on others. They also

---

[22] Ibid, 25-26.

[23] Brian Orend, 'JUST POST BELLUM: A JUST WAR THEORY PERSEPECTIVE,' in *Jus Post Bellum*, 33.

[24] See Human Security Report 2005, *The Changing Face of Global Violence*, 53. Ironically, studies indicate that nationwide mortality rates overall appear to be dropping as well.

Several interrelated long-term changes have been driving this counterintuitive development:

i) The average war today is fought by smaller armies and impacts less territory than conflicts of the Cold war era. Smaller wars mean fewer war deaths and less impact on nationwide mortality rates.

ii) Dramatic long-term improvements in public health in the developing world have steadily reduced mortality rates in peacetime-and saved countless lives in wartime.

iii) Major increases in the level, scope, and effectiveness of humanitarian assistance to war-affected populations in countries in conflict since the end of the Cold War have reduced wartime death tolls still further.

Human Security Report 2009, *The Shrinking Costs of War*, 1-3.

[25] A standard definition is as follows:
(adj) moral (concerned with principles of right and wrong or conforming to standards of behavior and character based on those principles) 'moral sense'; 'a moral scrutiny'; 'a moral lesson'; 'a moral quandary'; 'moral convictions'; 'a moral life.' wordnetweb.princeton.edu/perl/webwn, *retrieved at* http://wordnetweb.princeton.edu/perl/webwn?s=moral, 04/03/2010.

[26] *See generally*, James Turner Johnson, *The Just War Tradition and the Restraint of War* (Princeton, NJ: Princeton University Press, 1981); Walzer, *Just and Unjust Wars.*

[27] Orend, *War,* 5-9; *see also*, Dinstein, *War, Aggression and Self-defense*, 63-71.

provide *legitimacy* for the actor in that the violence can be said to be *minimally just.*

Even if a war is determined to be *just*, there are constraints on how the war *ought* to be fought (*Jus in bello).* A just actor must project violence within the constraints of morally acceptable behavior in order to insure that the violence is projected only on those who are identified as participating in the war with that degree of force necessary to accomplish the tactical and strategic tasks necessary to accomplish the just goals of the conflict. Terms such as *military necessity, discretion,* and *proportionality* in the use of violence help to frame this discussion. An actor, then, can be justified in the decision to project force and yet become an unjust actor by the manner in which it prosecutes that projection of force. Interestingly, there is a disturbing thread in Just War Theory that deemphasizes the rules regarding the conduct of war and emphasizes the reasons for going to war. The term *jus in bello*, for example, has little currency before the Enlightenment and really only moves to the forefront in the twentieth century.[28] There is an argument that ignores, or at least deemphasizes, the methodologies of war in the furtherance of a just cause. This argument implies that 1) if an actor's cause is *just*, it should not be constrained as to how it fights[29]; and 2) the best way to bring a just war to an end is to direct all necessary force towards the destruction the *unjust* enemy's ability to fight.[30] *Jus in bello* conduct has received most of its articulation as it became conflated with international law principles discussed below.

Just War theory does speak to the outcome of wars when it requires actors, as part of their calculus regarding the projection of force, to determine that the results reflect '…at least a *proportionality* of benefits to costs.'[31] In order to make this determination, however, the question must be answered what is the purpose of a just war? How does one know whether the results are *so* terrible as to render the original purposes of the projection of force unjustified? Some traditionally have answered that the purpose of a just war is to reestablish the *status quo ante bellum,* that set of circumstances which existed before the war began. Waltzer, and others, disagree and argue for a result which is more secure and which reflects a more just state of affairs than existed before the war began.[32] The rights of a community which have been violated and thus justify the use of force in defense of those rights should, it is argued, at the least, be capable of vindication. This formulation, of course, constrains the aggrieved party from taking actions which do more than vindicate rights lest that actor become an aggressor-unjust actor- as well. This is consistent with the overall purpose of just war theory, that being the setting of moral constraints on the aims, conduct, and results of war.[33]

International Law (IL).

With the growth of the nation-state system, IL has come to the forefront in order to answer the important questions and regulate the conduct of war. First, it must be emphasized that IL is *positivist* rather than *normative;* it speaks, at its best, to the utilitarian purpose of making

[28] As one commentator notes:

> …neither term [*just ad bellum* or *jus in bello*] can be found in the texts produced by other major publicists during the interwar years, nor, according to our investigations, were they used in the courses on war and peace given at the Hague Academy of International Law or in any other courses. The breakthrough occurred only after the Second World War, when Paul Guggenheim, another disciple of the School of Vienna, drew the terminological distinction in one of the first major international law treatises of the postwar era. A number of monographs subsequently took up the terms, which soon gained widespread acceptance and were launched on their exceptionally successful career. In a thesis written under Guggenheim's supervision and published in 1956, Kotzsch gave them pride of place, treating them in a manner to which we have grown accustomed and which we now take for granted.

Robert Kolb, "Origin of the Twin Terms just ad bellum/jus in bello." *International Review of the Red Cross,* 1997 no. 320, 555 retrieved at http://www.icrc.org/web/eng/siteeng0.nsf/iwplist163/d9dad4ee8533daefc1256b66005affef, 03/31/2010.

[29] Ian Clark puts the question this way:

> In a case where it is believed that there is only one just party to the conflict, that is, one party whose cause is just, why should that party be restrained in its prosecution of the war in the same manner as the unjust party? Since war is not a game, and we are not indifferent to its outcome in devising the rules which govern it, why should we prejudice the result by expecting the party which is fighting for a just cause to fight in such a way that it may lose?

Ian Clark, *Waging War: A Philosophical Introduction* (Oxford: Oxford University Press, 1990) 36.

[30] These arguments continue to have currency in the 21st century. Michael Gross, for example notes:

> …there is preliminary evidence that targeted killings, aggressive interrogation, nonlethal weapons, and attacks on participating civilians (by either side) reflect emerging norms of warfare. Whether these norms are new rules or acceptable exceptions, they are far from the prohibitions and severe restrictions that currently characterize the laws of war.

Gross, *Moral Dilemmas of Modern War,* 238. *See also* General Colin Powell's proscriptions regarding the use of force wherein he contended that forces should only be deployed when national interest, commitment, and support have been established, but then there should be use of overwhelming force in the military encounter-rather than proportional response. Regarding the Iraqi Army in 1991, for example, he noted the war aim, 'first we're going to cut it off, then we're going to kill it.' Doug DuBrin, 'Military Strategy: POWELL DOCTRINE, Background, Application and Critical Analysis,' *Newshour Extra, retrieved at* http://www.pbs.org/newshour/extra/teachers/lessonplans/iraq/powelldoctrine_short.html, 03/31/2010; Ruth Wedgwood *Legal and Ethical Lessons of NATO's Kosovo Campaign* (Newport, Naval College 2002) ,434-435; and Sharma, "Chapter 1 RECONSIDERING THE JUS AD BELLUM/JUS IN BELLO DISTINCTION," 28-29.

[31] Brian Orend, "Justice after War," *Ethics and International Affairs*, v. 16.1 (Spring 2002).

[32] Waltzer, *Just and Unjust Wars,* 119.

[33] Orend, "Justice after War," 46.

man-made rules which aid mankind in the conduct of war. It does not speak to what *ought* to be appropriate behavior amongst actors; rather it provides minimal standards of conduct which are adjudged by the community of international actors to be in their interest and to be useful in the constraint of the project of war. It assumes that war will occur and seeks to criminalize behavior in order to protect, where possible, the potential for peaceful relations. It is not *universal* except to the extent that all actors agree to its terms and it is not *immutable* because it accepts changes to the rules as the international community deems them appropriate through treaty agreements or customary practice.[34] As Carsten Stahns notes:

> Moral theory and legal science share distinct origins and rationales and approach the relationship between jus ad bellum, jus in bello and jus post bellum from different angles. Moral philosophy is primarily concerned with the moral justification of warfare, under which the operation of the principles of jus ad bellum, jus in bello and jus post bellum is closely connected to the overall (just or unjust) cause of the recourse to force. International lawyers, by contrast, tend to view each of these categories as autonomous rules of behavior, with the aim of maximizing compliance and respect for human dignity. It is therefore not contradictory to construe jus post bellum differently in each discipline.[35]

IL has, however, become conflated with just war principles as well as a whole host of other articulated human rights articulations. Just war theorists, then, are often bogged down in suggesting best practices for actors which will be *useful* and IL commentators are often heard to speak in terms of *what* is *fair and right.*[36]

The history of IL as it pertains to war is instructive. As nation-states eschewed normative and theological justifications for their existence and actions in the 17th and 18th centuries, states accepted their right to conduct war as a responsibility of statehood. The justice of a state's cause in the projection of force, then, lost a good deal of its validity; rather states conducted war as a matter of right in the exercise of their responsibility to pursue national policy.[37] How war was to be conducted, however, began to take preeminence, reflecting as it did age-old customary practices of warriors in the field. Purely utilitarian concerns abounded; treatment of fallen soldiers, prisoners of war, uninvolved civilians, destruction of non-military targets, use of new technologies. This movement acknowledged that *de facto* wars would continue but that if they were conducted in a particularly barbaric manner, the peaces to be obtained would not last. Revenge, rising out of the ashes of a particular conflict, might well stoke the fires of the next conflict, especially where armies were becoming democratized and ideological, and states lost the ability to turn the violence on and off at will. Thus, the exhortations of Abraham Lincoln during the American Civil War that

> [w]ith malice toward none; with charity for all; with firmness in the right, as God gives us to see the right, let us strive on to finish the work we are in; to bind up the nation's wounds, to care for him who shall have borne the battle, and for his widow, and his orphan-to do all which may be achieved and cherish a just and lasting peace among ourselves, and with all nations.[38]

A similar exhortation signed in St. Petersburg in 1868 recognized the purposes of war and the need to restrict certain weapons based on the following considerations:

> Considering that the progress of civilization should have the effect of alleviating as much as possible the calamities of war:
>
> That the only legitimate object which States should endeavor to accomplish during war is to weaken the military forges of the enemy;
>
> That for this purpose it is sufficient to disable the greatest possible number of men;

[34] A standard definition reads as follows:

> [L]aw is that element which binds the member of the community together in their adherence to recognized values and standards. It is both permissive in allowing individuals to establish their own legal relations with rights and duties, as in the creation of contracts, and coercive, as it punishes those who infringe its regulations…
> The rules of international law must be distinguished from what is called international comity, or practices such as saluting the flags of foreign warships at sea, which are implemented solely through courtesy and are not regarded as legally binding. Similarly, the mistake of confusing international law with international morality must be avoided. While they may meet at certain points, the former discipline is a legal one both as regards its content and its form while the concept of international morality is a branch of ethics. This does not mean that international law can be divorced from its values.

Malcolm N. Shaw, *International Law,* 6th ed. (Cambridge: Cambridge University Press, 2008), 2.

[35] Stahn, "Chapter 5, Jus Post Bellum: Mapping the Disciplines" in *Just Post Bellum*, 112.

[36] Jack L. Goldsmith, Erick A. Posner*, the Limitations of International Law* (Oxford: Oxford University Press, 2005), 14-17.

[37] Thomas W. Smith, "The New Law of War: Legitimizing Hi-Tech and Infrastructural Violence" *International Studies Quarterly,* v. 46, n. 3 (Sep., 2002) ,358-59; Kolb, "Origins of the twin terms just ad bellum/jus in bello," 554; James Turner Johnson, "The Just War Idea: The State of the Question," *23 Social Philosophy & Policy* (2006).

[38] Abraham Lincoln's Second InauguralAddress (March 4, 1865) *retrieved at* http://libertyonline.hypermall.com/Lincoln.lincoln-2.html, 03/31/2010.

> That this object would be exceeded by the employment of arms which uselessly aggravate the sufferings of disabled men, or render their death inevitable;
>
> That the employment of such arms would, therefore, be contrary to the laws of humanity…[39]

Thereafter, Conventions of various kinds and with various participants occurred to address a myriad of issues including what was called the *law of land warfare.* Through the Hague Conventions of 1899 and 1907 and the Geneva Conventions of 1864, 1928, 1929, 1949 and 1975, an extremely robust set of rules and proscriptions regarding conduct were enacted and ultimately agreed upon in part by most states forming the international community. Aligned with but separate from a set of rules dealing with personal human rights, this body of law has been denominated *international humanitarian law* (IHL). There are enforcement mechanisms as well including originally the Nuremburg Court system, multiple international courts and ultimately the International Criminal Court.[40]

On a separate track, and primarily as a result of the catastrophes of World Wars One and Two, IL developed a response to the question regarding the justification for an actor's projection of force. Indeed, IL went well beyond the reasoning of just war theory and attempted to outlaw war altogether. Beginning with the League of Nation's Charter, through the Kellogg-Briand Treaty and finally the United Nation's Charter, IL outlawed war between states except in situations of self-defense or where the international community, through the U.N. Security Council, sanctioned it.[41]

Like all systems of constraint, especially on the international stage where there are minimal means to enforce proscriptions, IL has had its failures.[42] It struggles, for example, with the reality that all actors are not sovereign states and that evolving definitions of *war* are rarely covered by its articulations. Further, in a globalized world, conflicts that have previously been considered *domestic* now clearly affect the entire global community.[43] As Bill Nash, the American General responsible for peacekeeping operations in Bosnia-Herzegovina, noted, '[T]he first rule of nation-building is that everything is related to everything, and it's all political.'[44] An entire human rights regime has grown up since World War Two, which demands vindication not only of state's rights but also individual rights during and after war is conducted and there is a growing recognition that economic and social rights are entitled to equal pride of place with political and security rights. Finally, there are a whole host of actors who refuse to pay even lip service to the proscriptions of IL as they conduct force projection on the international stage. Post War conduct of actors is rarely addressed in IL. There are some discussions about the Responsibility to Protect (R2P)[45] and a fairly robust set of IL requirements for states in the law of belligerent occupation, but these have not found their way into binding treaties or custom or apply to only a very discreet set of circumstances.[46]

---

[39] Declaration of St. Petersburg: November 29, 1868 *retrieved at* http://avalon.law.yale.edu/19th_century/decpeter.asp, 04/02/2010.

[40] *See, for example*, Richard J. Goldstone, *For Humanity, Reflections of a War Crimes Investigator* (New Haven, Ct.: Yale University Press, 2000); Omer Bartov, Atina Grossman, Mary Nolan ed. Crimes of War, *Guilt and Denial in the Twentieth Century* (New York:The New Press, 2002); Gary Johnathan Bass, *Stay the Hand of Vengeance, The Politics of War Crimes Tribunals* (Princeton, NJ: Princeton University Press, 2000).

[41] The UN Charter reads in pertinent part:

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore peace and security.

Charter of the United Nations, CHAPTER V11: ACTION WITH RESPECT TO THREATS TO THE PEACE, BREACHES OF THE PEACE, AND ACTS OF AGGRESSION, Article 51 (1945) *retrieved at* http://www.un.org/en/documents/charter/chapter7.shtml, 03/30/2010.

[42] Goldsmith, *the Limitations of International Law,* 225-26; David Kennedy, "The International Human Rights Movement: Part of the Problem?" *Harvard Human Rights Journal* v.15 (Spring 2002).

[43] *See for example*, G. R. Lucas Jr., "From *Jus ad bellum* to Jus Ad Pacem: Rethinking Just War Criteria for the use of Military Force for Humanitarian Ends," in D. Chatterjee and D. Scheid (eds), *Ethics and Foreign Interventions* (Cambridge, Cambridge University Press, 2003).

[44] Nash, *quoted in* Orend, "Jus Post Bellum: A Just War theory Perspective,'" *in Jus Post bellum*, 48.

[45] The responsibility to Protect (R2P) Doctrine appears to be an emerging norm which requires that when a state is either unwilling or unable to fulfill its responsibility to protect its own populations, UN members are obligated to take action to minimize human suffering. Most important, it involves the responsibility to prevent such atrocities from occurring, and if prevention fails, it requires states to react and rebuild. *See generally*, Gareth Evans, *the Responsibility to Protect: Ending Mass Atrocity Crimes Once and For All* (Washington D.C.: Brookings Institution Press, 2008).

[46] *See generally*, Yoram Dinstein, *The International Law of Belligerent Occupation* (Cambridge: Cambridge University Press, 2009).

> The authority of an Occupying Power is not derived from the will of the people, and democracy is not of any functional relevance to the running of an occupied territory. Belligerent occupation is not designed to win the hearts and minds of the local inhabitants; it has military-or security-objectives, and its foundation is the 'power of the bayonet.' The jurisdictional rights of the military government in an occupied territory…stem from effective control alone. LOIAC [The Law of International Armed Conflict] offers the inhabitants of the territory vital safeguards against possible maltreatment by the Occupying Power. But belligerent occupation must be acknowledged for what it is and for what it is not. 35.

Realism

While realism has had many twists and turns in its explanations over the years, for purposes of this paper it can be said that the doctrine has two purposes 1) to provide an explanation regarding how actors, especially states, act on the international stage and 2) to explain a set of assumptions upon which realist statesmen operate when they make decisions about when to go to war, how to conduct war, and how wars end. The doctrine has a long history ranging from Thucydides, Machiavelli and Hobbes to Hans Morgenthau, George Kennan, Reinhold Niebuhr, Henry Kissinger and Kenneth Waltz. Traditional realism speaks to power and security issues, the ability of states to survive and prosper in an anarchical world. Realists assume the appropriateness of war *if and only if* it is necessary to obtain a *national interest* and find it unreasonable for states to constrain themselves regarding the tools used to conduct wars or the ways that wars should end. Constraints and responsibilities found in just war theory and IL hold little cachet when measured against the absolute requirement for states to survive and prosper. The logic of Hobbe's dictum *Bellum omnium contra omnes,* the war of all against all, is often cited by realists to describe the state of the international community where there is no overarching governance to reign in the natural requirements of states to survive, one against the other.[47]

There is a strain of realism, however, that speaks to the efficacy of restraints in war. In a globalized international environment where states find it more and more difficult to operate unilaterally, there is an interest in developing *soft* as well as *hard* power in order to survive and prosper. Charles Krauthammer, for example, notes the problem when dealing with the domestic political debate between realists [conservatives] and idealists [liberals] in the United States:

> But here we come up against the limits of realism: You cannot live by power along. Realism is a valuable antidote to the woolly internationalism of the 1990s. But realism can only take you so far.
>
> Its basic problem lies in its definition of national interest as classically offered by its great theorist, Hans Morgenthau: interest defined as power. Morgenthau postulated that what drives nations, what motivates their foreign policy, is the will to power-to keep it and expand it.
>
> For most Americans, will to power might be a correct description of the world-of what motivates other countries-but it cannot be a prescription for America. It cannot be our purpose. America cannot and will not live by *realpolitik* alone. Our foreign policy must be driven by something beyond power. Unless conservatives present ideals to challenge the liberal ideal of a domesticated international community, they will lose the debate.
>
> Which is why amongst American conservatives, another, more idealist, school has arisen that sees America's national interest as an expression of values.[48]

In essence, there are benefits to cooperation – to the adherence to multilateral organizations and international law regimes – which are either too difficult to obtain or which cannot be obtained in a unilateral fashion. Going to war within the framework of UN constraints, conducting war within the legal proscriptions of the various Conventions, and even finishing a war by a long and expensive round of nation-building and development aid all have ramifications which unilateral action often cannot produce. Joseph Nye argues that *soft power*, which arises from the attractiveness of a country's culture, political ideals, and policies, is the ability of a state to persuade other states and actors to share its objectives or desired outcomes.[49] Adherence to restraints regarding conduct during war, for example, often benefits soldiers on the ground; adherence to treaties which ban certain types of weapons such as weapons of mass destruction can aid in the security of the domestic and foreign battlefield; and ensuring that states who have lost wars are able to reenter the international community on terms beneficial to both the victor and the defeated can lessen the possibility of war for the next generation. For realists, adherence to these restraints is not based on the *normative* philosophy of how states *ought* to act, nor is state conduct restrained by the legalisms of IL. Rather, adherence is based on the assumption that cooperation with other states coupled with *hard* power is in the national interest, leading to the state's ability to provide security and prosperity for its citizens.[50]

Pacifism

Pacifism is a doctrine which objects to war outright, specifically to the kinds and degrees of violence that war involves, e.g. mass killing for political reasons. It references Gandhi's campaign against the British in India in the 1940's and Martin Luther King Jr.'s non-violent

[47] Victor Hanson, *Carthage and Culture: Landmark Battles in the Rise to Western Power* (New York: Random House, 2002); Henry Kissinger, *Diplomacy* (New York: Simon & Schuster, 1994); Stephen M. Walt, "International Relations: One World, Many Theories,"*Foreign Policy*, n. 110 (Spring 1998); H. J. Morgenthau, *Politics among Nation,* 7th ed. (New York: McGraw-Hill Companies, 2005); K.enneth Waltz "Realist Thought and Neorealist Theory," in *Controversies in International Relations Theory: Realism and the Neoliberal Challenge,* ed. Charles Kegley (New York: St. Martin's Press, 1995); John Mearsheimer, "The False Promise of International Institutions," *International Security* 19:3 (Winter 1994-95).

[48] Charles Krauthammer, "Democratic Realism, An American Foreign Policy for a Unipolar World*,"* (Washington D.C. 2004) , 13.

[49] Joseph Nye, Soft *Power: The Means to Success in World Politics* (New York: Perseus Books Group, 2004), 5-6.

[50] Krauthammer speaks in terms of democratic realism, for example:

> And this is its axiom: We will support democracy everywhere, but we will commit blood and treasure only in places where there is a strategic necessity-meaning, places central to the larger war against the existential enemy, the enemy that poses a global mortal threat to freedom.

Krautheimer, "Democratic Realism," 16.

civil rights activities in the 1960s. It proposes that war is such a terrible human activity that it should be outlawed in all its forms and argues that the other theories which purport to constrain its conduct are routinely manipulated and distorted to make their restraints meaningless. Finally, it implores individuals to renounce the use of the projection of force as a matter of conscience. There is a long Eastern, as well as Western, tradition of the doctrine, in addition to religious and secular justifications for its arguments. In its purest form, however, it can be said that pacifism rejects any argument for the projection of force by states or other actors. It, therefore, does not need to concern itself with conduct during war or obligations which may attend the victor.[51]

THE RIGHT WAY TO END A WAR

Given the discussion above, it may be concluded that there is *no one right* way to end a war. The wide divergence in the justifications for the projection of force, e.g. response to a terrorist event or invasion of a state, for example; the nature of the conflict, e.g. conventional or unconventional asymmetric warfare; the practices used to prosecute the war, e.g. targeted killing, enhanced interrogation techniques or strict compliance with the *jus in bello* requirements of international humanitarian law (IHL) by one or both sides; and the manner in which the conflict is concluded, swift capitulation by a state, regime change, continued insurgency, aggressor victory etc. These and multiple other variables influence how the parties will act *post bellum*. And yet, the manner in which a conflict is concluded can make all the difference.

Principles regarding *jus post bellum* are at present incomplete and subject to considerable argument,[52] yet the basic premise, found in *jus ad bellum* seems to apply. Before states can *morally* project force they must determine the *proportionality* of the results, that is does the foreseeable end outweigh the damage which the projection of force will inevitably cause? This just war theory requirement seems to imply that conflict can only be initiated where an actor determines that the end result will be less traumatic, especially to the innocent who will be affected, than the benefits to be obtained. There is a further implication here; should an actor determine the necessity for conflict, it must be prepared to, and indeed has a *moral* obligation to, right the economic, social, and political trauma which its conflict will create.[53]

Brian Orend asks the question, what are the ends or goals of a just war? He provides the following answer:

> The general answer is a more secure possession of our rights, both individual and collective. The aim of a just and lawful war, we know, is the resistance of aggression and the vindication of the fundamental rights of societies, ultimately on behalf of the human rights of their individual citizens. These values revolve around the concept of a minimally just and hence legitimate community. Such a community is one which does all it reasonably can to: (i) gain recognition as being legitimate in the eyes of its own people and the international community: (ii) adhere to basic rules of international justice and good international citizenship, notably non-aggression: and (iii) satisfy the human rights of its individual member (to security, subsistence, liberty, equality and recognition.[54]

He suggests a number of principles which would be '….at least permissible with regard to a just settlement of a just war': (1) Rights vindication, (2) Proportionality and publicity, (3) Discrimination, (4) Punishment, (5) Compensation and (6) Rehabilitation.[55] He goes on to suggest some concrete guidance in order to affect a just result.

> 1. Adhere diligently to the laws of war during the regime take-down and occupation;
> 2. Purge much of the old regime and prosecute its war criminals;
> 3. Disarm and demilitarize the society;
> 4. Provide effective military and police security for the whole country. Work with a cross-section of locals on a new rights-respecting constitution which features checks and balances;
> 5. Allow other, non-state associations, or 'civil society,' to flourish;
> 6. Forego compensation and sanctions in favor of investing in and re-building the economy;
> 7. If necessary, revamp educational curricula to purge past propaganda and cement new values;
> 8. Ensure that the benefits of the new order will be; (i) concrete; and (ii) widely, not narrowly distributed; and

---

[51] *See, for example* M. Ghandi, *Non-Violence in Peace and War, 1942-1949* (New York: Garland Publishing, 1972); Martin Luther King, *A Testament of Hope: the Essential Writing of Martin Luther King, Jr. ed*. J. Washington (New York: HarperOne, 1990); Bertrand Russell, "The Future of Pacifism,"*The American Scholar* (13: 7-13 1943); Jenny Teichman, *Pacifism and the Just War* (Oxford: Oxford University Press, 1986).

[52] M. Freeman, D. Djukie, "Chapter 11, JUST POST BELLUM AND TRANSITIONAL JUSTICE," in Stahn et al eds. *Jus Post Bellum,* 224. *See also* T. Seybolt, *Humanitarian Military Invention, The Conditions for Success and Failure* (Oxford: Oxford University Press, 2008).

> A great deal of ink has been spilled on this topic [human security as a justification for military intervention] already, much of it by international lawyers and moral philosophers whose legal and moral debates have shifted ground considerably since the end of the Cold War but whose arguments remain in a state of 'vincible ignorance' of empirical support. p.3.

See also, J. L. Holzgrefe, Robert Keohane *eds. Humanitarian Intervention: Ethical, Legal and Political Dilemmas* (Cambridge: Cambridge University Press, 2003).

[53] Michael Waltzer, "Just and Unjust Occupation," *Dissent* (Winter 2004) and "Regime Change and Just War," *Dissent* (Summer 2006); Sharma, "RECONSIDERING THE JUS AD BELLUM/ JUS IN BELLO DISTINCTION," in *Just Post Bellum,* 29.

[54] Orend, 'JUS POST BELLUM: A JUST WAR THEORY PERSPECTIVE,' in *Jus Post Bellum,* 39.

[55] Ibid, 40-45.

> 9. Follow an orderly, not-too-hasty exit strategy when the new regime can stand on its own two feet.[56]

Anyone who has spent any time working at peace-keeping, peace-making, nation-building or the provision of humanitarian aid knows that the devil is in the details. The above represent a fair checklist of discreet areas to be addressed should one actor intend to involve itself in the project of wholesale transition of a society from one set of values and political mechanisms to another. These are not inexpensive undertakings. As U.S. actions in Iraq and Afghanistan have demonstrated, accomplishing the above goals can take decades, contribute to multiple additional deaths and destruction and cause cultural collisions, which may never be healed. They represent, one might argue, very Western constructions of what a minimally just society *ought* to look like. Finally, they are open to the criticism that the enumerated responsibilities are akin to requiring actor A, who has been assaulted by actor B, to pay not only for the court proceedings used to vindicate his rights, but the psychological counseling necessary to cure the malady that caused actor B to act-out in the first place. Yet, the question remains, is an actor which has prosecuted a just war required to undertake these types of activities in order to be judged *moral*? Ethicists have yet to come to a consensus on this issue.[57]

To date, international law does not specifically address conduct, post bellum, except in the area of IHL. Here, parties to conflicts argue that their ability to regulate the conduct of actors post-conflict is limited by the conditions on the ground, the emergent and often chaotic nature of the environment, the breakdown in civil authority, the lack of resources to create a robust civil society and other legal and actual constraints. There is considerable disagreement as to whether occupiers are bound to enforce the expansive human rights found in the various human rights treaties that bind, generally, signers of these treaties to treatment of individuals within their jurisdictions.[58] And international criminal courts, as a rule, restrict their prosecutorial jurisdiction to *grave* breaches of IHL, leaving lesser breaches of IHL to the domestic criminal codes of actors. Yet occupiers, in a general sense, are staying longer, projecting force in and among civilians, and assuming responsibilities for the administration of civil society that were not originally contemplated by IHL. This legal *black hole* has been described by Charles Garraway as follows:

> But not only are the actors on the battlefield changing, so is the battlefield itself. Soldiers are no frequently involved in post-conflict situations where the international rules are far from clear. What is the entitlement to use force during a period of occupation? Do 'combat rules' apply [IHL] or have we moved to a more threat based regime? And what is the position where 'major combat operations' may have ceased but violence persists? In Helmand province, some years after the initial intervention, United Kingdom and other NATO forces have been involved in what one senior officer described as the most intense fighting since the Korean War. But what law applies to the actions of those soldiers? On what basis are targeting decisions taken? The stark difference between status based and threat based legal regimes causes inevitable difficulties when operating in the grey area that is post-conflict…Indeed does the Convention-or the International Covenant on Civil and Political Rights-even apply in situations of this nature where troops are operating outsides their national boundaries? These are issues over which there is strong disagreement, particularly within the United States, and yet for members of the armed forces, they are critical. They may represent the difference between a gallantry medal and a prosecution for murder.[59]

While the realist tradition might well embrace Colin Powell's maxim that an immediate and clean exit strategy after the projection of force is appropriate to the vindication of the national interest, the reality on the ground is that in a globalized international environment definitions of national interest are less clear than they have been in the past and the ramifications of force projection, no matter how small, affect multiple sets of international actors now and in the future. What is the national interest, for example, for the invasion of Iraq? There are multiple answers. One might be the destruction of Saadam Hussein's ability to foster international terrorism and the proliferation of weapons of mass destruction. Another might be regime change in order to ensure that this particular dictator could no longer play havoc with the regional political order and thus disrupt the free-flow of energy, etc. A third interest might be the creation of the first Arab democracy in order to begin the development of a reasonably secure and peaceful region. Each of these tasks requires different levels of force projection, time-tables and commitments of blood and treasure. The same analysis holds for force projection in Sierra Leone, Bosnia-Herzegovina, the Democratic Republic of Congo, Rwanda, or Sudan.

---

[56] Ibid,45-49.

[57] Interestingly, Orend moves beyond the question of morality and into the field of utility (realism?) and international law as he describes the above responsibilities.

> I reply that war-winners, war-losers and the international community could all profit from clear standards, guidelines and benchmarks for behavior in difficult post-war scenarios. It is in all our interests to regulate behavior in post-war moments, and to channel it in the direction of minimal justice and political legitimacy. 52.

[58] Ralph Wilde, "ARE HUMAN RIGHTS NORMS PART OF THE JUST POST BELLUM, AND SHOULD THEY BE?" in *Jus Post Bellum.*

> The question of the applicability of international human rights norms to situations of foreign occupation/administration, thereby forming part of the *jus post bellum* is as important as it is under-evaluated. 185.

[59] Charles Garraway, "THE RELEVANCE OF JUS POST BELLUM: A PRACTIONER'S PERSPECTIVE," in *Jus Post Bellum,* 157.

How to use force, it is recognized, also carries with its ramifications for the future as well. No longer is the mission of the infantry always to 'close with and destroy the enemy.' The U.S. Army's Field Manual regarding the proper application of force notes:

> Section V1-Rules of Engagement 2-66 The proper application of force is a critical component to any successful counterinsurgency operation. In a counterinsurgency, the center of gravity is public support. In order to defeat an insurgent force, US forces must be able to separate insurgents from the population. At the same time, US forces must conduct themselves in a manner that enables them to maintain popular domestic support. Excessive or indiscriminant use of force is likely to alienate the local populace, thereby increasing support for insurgent forces. Insufficient use of force results in increased risks to US and multinational forces and perceived weaknesses that can jeopardize the mission by emboldening insurgents and undermining domestic popular support. Achieving the appropriate balance requires a thorough understanding of the nature and causes of the insurgency, the end state, and the military's role in a counterinsurgency operation.[60]

The lesson here is that while all politics is local, increasingly all politics is international as well; especially for those, like the United States, which benefit the most from the interconectiveness of the global economic environment.

How to Judge a Successful End to Conflict?

While *just war theorists* seek conditions in a *post bellum* environment which outweigh the harms caused by war (constraints on starting a war) and *international law* speaks primarily to the conduct of actors in war, it may be the *utilitarians* or *realists* that stretch the continuum of responsibilities required of victors in the future (after the war).

Redefining national interest, then, may well require leaving the battlefield in a state that will not require a return for the next generation; cleaning up the battle space of weapons, setting conditions for security and economic growth, and insuring that those left behind are capable of joining the international community with a degree of domestic tranquility that permits global integration. Since these projects take time, hasty judgment adds little to meaningful analysis. Actors who would wage war need to remember, however, that war, no matter how it is defined, has never been cheap. Yet in a global world, the price of a failed peace can be even more expensive.

[60] FMI 3-07-22 Counterinsurgency Operations *retrieved at* http://www.fas.org/irp/dodir/army/fm13-07-22.pdf, 04/02.2010.

Shedding New Light on North Korea's Nuclear Ambitions

Nellwyn Olson

I. Introduction

As the United States confronts new and ever evolving security threats with innovative and adaptive thinking, there is one security threat that has persisted for almost a quarter of a century and has been met with repetitive alarms and cyclical reactions: the North Korean nuclear threat. Almost a decade ago, U.S. relations with North Korea were on an upswing with the October 2000 Joint communiqué expressing mutual interest in achieving peace and security; North/South Korean relations were even significantly improved with the first inter-Korean summit in June of that year. The stark contrast with the current relations with North Korea demonstrates the fluctuating, but ever present task of confronting North Korea nuclear threats. Solutions over how best to deal with North Korea have ranged from military intervention, United Nations Security Council sanctions, bilateral and multi-lateral negotiations, to stick-and-carrot offerings. The dialogue over North Korea's nuclear issue has reignited after each nuclear test or discovery and has often led to equating North Korean nuclear endeavors with the production of nuclear weapons.

Siegfried Hecker's[1] most recent visit to North Korea's Yongbyon site in November 2010 reignited controversies over the country's nuclear ambitions and nuclear weapons program. As one of the world's most demonized countries, North Korea's endeavors often occasion analysts' worst-case scenarios and the international community's stick-and-carrot treatment. Whether North Korea deserves this reputation is open to interpretation which will not be addressed in this paper. Perceptions regarding North Korea are problematic however, when they are derived from over-generalized assessments, intuitive leaps, and preconceived expectations. This paper seeks to articulate a more nuanced assessment of North Korea's current nuclear program by highlighting how common and problematic intuitive leaps create obstacles for an accurate evaluation of North Korea's nuclear capabilities and can harm future negotiations.

II. The North Korean Nuclear Threat

There is no denial that North Korea's nuclear capabilities pose a threat to North East Asia's security. Because of the limited availability of knowledge on North Korea's nuclear program, there is debate over exactly what type of threat and how much of a threat their programs pose. The distinction between North Korea's capacity, capability, and completed construction of nuclear weapons becomes lost as discussions focus on the number of nuclear bombs that North Korea can produce; identifying these distinctions will be critical to defining points of friction or opportunities for negotiations.

History of North Korea's Nuclear Program

The source of North Korea's nuclear threat has often been linked to the country's capabilities and intentions to produce nuclear weapons, and their past nuclear and missile tests. Although it is difficult to concretely identify North Korea's nuclear intentions, the country's past actions warrant concern over the current capacities for nuclear weapons development and proliferation.

North Korea's membership to the Nuclear Non-Proliferation Treaty (NPT), from 1985 through 2003, has been an opportunity for some international oversight over the country's nuclear programs. During this time, International Atomic Energy Agency (IAEA)[2] inspections have uncovered inconsistencies and attempted deceptions by North Korea that have increased suspicion that North Korea was diverting fissile material to develop nuclear weapons. In 1990, IAEA testing of North Korea's fuel rods for its 5Mwe gas-graphite reactor indicated the possibility or three different episodes of plutonium separation between 1989 and 1991, which contradicted North Korea's claim of a single episode of plutonium separation in 1990. One of the IAEA inspectors stated, "We had to approach [North Korea] harder and harder as they realized we were going to discover their wrongdoings."[3] During this period, according to IAEA officials, there was also evidence of North Korea attempting to hide or camouflage facilities of particular interest to the IAEA inspectors.[4] According to Oberdorfer, the North Korean "minister of atomic energy, Choi Hak Gun, told IAEA inspectors, 'Even if we had done it [cheated], we would never admit it.'"[5]

The IAEA's difficulty in accounting for North Korea's past nuclear history had furthered the speculation on possible attempts by North Korea to develop nuclear weapons. Such speculation was later in line with the country's nuclear weapons tests on October 9, 2006 and May 25, 2009. North Korea's, as Hecker describes, "limited and less-than-successful

[1] Siegfried Hecker served as director of Los Alamos Laboratory from 1986-1997 and is currently a Co-Director of the Center for International Security and Cooperation and Professor at Stanford University. Hecker has made several visits, in an unofficial capacity, to the North Korean nuclear complex.

[2] The IAEA is an independent international organization that works closely with the United Nations on several nuclear issues. The IAEA conducts inspections to verify that countries implement proper protocols and procedures as contained within the NPT.

[3] Don Oberdorfer, The Two Koreas. (Basic Books, 2001), 270-271.

[4] Ibid., 275.

[5] Ibid., 278.

nuclear test history," severely underwhelmed analysts worst-case-scenario estimates, however they did confirm observers expectations of the country's military nuclear ambitions.[6]

Current Concerns

Currently there is no IAEA oversight of North Korea's nuclear activities, as North Korea remains the only country to have withdrawn from the NPT. Any discussion of rejoining the NPT and IAEA inspections will likely be closely linked with Iran's obligations under the treaty. Iran is a current NPT member and claims to be developing a civilian nuclear energy program which has elicited international concern.[7] In addition, there are also concerns that North Korea may attempt to sell its nuclear technologies, fissile material, and/or its technical knowledge to countries and terrorists.

Given North Korea's past actions, it is understandable to react with suspicion and unease towards their most recent nuclear endeavors. However, if we view North Korea's actions in terms of the amount of bombs they can produce or the amount of technology and knowledge they are capable of proliferating, then overgeneralizations caused by fears can cause us to lose track of the more nuanced details. Such nuanced details will likely become obstacles to the resumption of six-party talks and bilateral negotiations or they can provide an opportunity for areas of mutual cooperation or at least international oversight on North Korea's nuclear activities.

III. The Facts of North Korean Nuclear Facilities

On November 12th, Siegfried Hecker, accompanied by John Lewis and Robert Carlin, traveled to the Yongbyon Nuclear Complex to observe North Korea's latest nuclear endeavors. Hecker's presents an objective analysis from his observations in his November 20, 2010 summary which will be briefly summarized below.[8]

Currently, North Korea is constructing an estimated 25-30MWe[9] Light Water Reactor (LWR)[10] which, according to North Korean officials, is a small prototype for a larger LWR to be built once the technology is mastered. A recently constructed uranium enrichment facility is reported to be operational and contain 2000 gas-centrifuges. These two facilities, according to Hecker, appear to be designed primarily for generating civilian nuclear power. As for previously known structures, the 5MWe gas-graphite reactor[11] appeared dormant but remained on stand-by mode while the 50MWe gas-graphite reactor continued to stand abandoned as a pile of iron and concrete.

Hecker provided a balanced and objective analysis of his findings by contrasting his views with possible outcomes. He expressed belief in North Korea's pursuit of nuclear electricity as genuine while balancing his assessments by citing the facility's capacity to amass a certain amount of weapons-grade nuclear material. In another example of Hecker's objective analysis, he noted that the 5MWe gas-graphite reactor is in stand-by mode, but could become operational within six months with reconstruction of the cooling tower. In addition, he compared the ease with which various facilities could be employed to produce fissile material while also comparing their civilian use capabilities.

IV. Media Coverage on North Korean Developments

Although some of Hecker's observations have been disseminated widely through recent commentary on North Korean nuclear developments, his objectivity and nuanced approach have largely failed to command the same attention. Following Hecker's most recent visit, a large portion of articles mentioned North Korea's uranium enrichment only when linked with fears of producing more bomb fuel. When media reports mentioned the North Korean stated goal of producing civilian power, it was often framed within the context of hiding more sinister ambitions.

In an article for Foreign Policy Magazine, Josh Rogin illustrates the popular view of North Korean initiatives as a cover for illicit activity:

> As tensions spiral upwards on the Korean peninsula, North Korea's construction of a light water nuclear reactor in addition to its new, sophisticated uranium enrichment facility, allows the regime to claim that its enrichment program is for domestic civilian power needs -- as [sic] the same argument that Iran makes -- according [to] the first Western scientist allowed to visit the facility.[12]

Many media reports have simply stopped mentioning the North Korea's stated pursuit of nuclear energy all together, and simply equated actions involving North Korean nuclear endeavors with the pursuit nuclear weapons.

The absence of any mention of dual-use technology and civilian nuclear endeavors invites unproven assumptions to become fact:

> With North Korea's choice to use centrifuges to enrich uranium to fuel its nuclear weapons, an axis of states that use the technology has now emerged with North Korea, Pakistan and Iran.[13]

[6] Siegfried S. Hecker, "Redefining denuclearization in North Korea," *Bulletin of the Atomic Scientists*. December 20.

[7] David Albright and Paul Brannan, "Taking Stock: North Korea's Uranium Enrichment Program." *The Institute for Science and International Security* (2010): 28.

[8] Siegfried S. Hecker, "A Return Trip to North Korea's Yongbyon Nuclear Complex," *Center for International Security and Cooperation of Stanford University* (2010).

[9] Megawatt of electricity (MWe): Measurement of electricity which is equivalent to 1000 watts of electricity.

[10] Light Water Reactors require low enriched uranium as fuel and use water as a moderator.

[11] Gas Graphite Reactors do not require enriched uranium, use natural uranium as a feed and use CO_2 or helium as a coolant, and graphite as a moderator.

[12] Josh Rogin, "Hecker: North Korea Now Has Same Nuclear Defense as Iran," *Foreign Policy Magazine* (2010)

[13] Christine Kim, "Getting a grip on the centrifuge subterfuge," *Korea JoongAng Daily,* November 23, 2010.

Countries with a stake in the protracted multinational efforts to denuclearize North Korea are crafting a concerted reaction, possibly including new sanctions, to the North's latest nuclear disclosure that it is equipping itself with another capability to produce nuclear weapons.[14]

With each new simplified equation captured by the popular discourse on North Korean endeavors, the public's and media's knee jerk reaction to North Korean activities becomes all the more solidified. With multi-lateral and bilateral discussions already "mired in distrust and accusations,"[15] achieving a consensus on North Korea's nuclear ambitions will likely be an obstacle in the pursuit of an overall agreement between the United States and North Korea.

V. Discussion in Detail

It is possible that North Korea could use the current uranium enrichment facilities or have additional hidden facilities that produce highly enriched uranium that they are stockpiling to create nuclear weapons. The link between North Korea's current endeavors and stockpiling nuclear bombs has been greatly oversimplified, and in my opinion, is tenuous at best. To provide some clarity on the current debate, further clarification on North Korea's nuclear endeavors will be discussed.

Prior North Korean Claims

Although many observers were taken by surprise on November 12, 2010 when the public learned about North Korea's efforts to build a light water reactor, North Korea had first announced its intentions in 2009 in response to UN sanctions. A North Korean spokesman issued a statement on April 29 that "the DPRK will make a decision to build a light water reactor power plant and start the technological development for ensuring self-production of nuclear fuel as its first process without delay."[16]

Siegfried Hecker's Reaction

Prior to Hecker's latest visit to the Yongbyon Complex, he did not believe that North Korea could achieve this goal on a large scale. In "North Korea's Choice: Bombs over Electricity," co-authored by Hecker, he explains "we believe that North Korea is not technically prepared to enrich uranium beyond the laboratory scale or to build its own LWR."[17] In several articles, Hecker's reaction is coupled with the description of thousands of centrifuges to paint a scene for an impressive and ominous endeavor. Such ominous descriptions are typical when describing North Korean nuclear endeavors, yet such figures should be put into perspective.

Civilian and Military Uses of Nuclear Technology

In current media reports, North Korea's recent construction of a prototype LWR and uranium enrichment facility has spurred fear of an increased capability for North Korea to acquire nuclear weapons. With nuclear enrichment facilities, it is relatively easy to transition from the production of low enriched uranium (LEU), which can be used to fuel nuclear reactors, to the production of highly enriched uranium (HEU), as used for the development of medical isotopes and nuclear weapons.[18] Concerns over increased capacity for nuclear weapons development derived from uranium enrichment have been focused predominantly on Iran and North Korea despite this quality being common to any country or company who engages in uranium enrichment. Using the same parts, highly enriched uranium can be achieved by rearranging the cascades (a specific arrangement of centrifuges) thus enabling the low enriched uranium to flow through a greater number of separation step.[19]

The ability to derive fissile material from dual-use technology, a trait common to all uranium enrichment facilities, has been so closely associated with North Korean endeavors that any pursuit of nuclear energy will likely face skepticism and alarm from the American perspective. The divergent perspectives between North Korean insistence on engaging in civilian nuclear power and the views of most analysts of North Korean ambition to increase its nuclear weapons capacity will likely provide considerable friction in present relations and future negotiations. Even outside of negotiations, North Korea's uranium enrichment facility has become a battleground of speculation over the presence of additional uranium sites, proliferation of enrichment knowledge, and other issues. Referring to U.S. initiatives against North Korea's enrichment facilities, chief non-proliferation advisor, Gary Samore, stated, "The U.S. and its allies are doing everything we can to try to make sure that we complicate matters for [North Korea]".[20] The dual-use characteristic common to all enrichment facilities has been forgotten or ignored when framed within the North Korean context.

Focus on Number of Centrifuges

The number of centrifuges has often been used as evidence to demonstrate the alarming size of the North Korea's nuclear facilities. On its own, the number of centrifuges does not provide a clear overview of North Korea's enrichment capabilities, yet the described

[14] Moon Gwang-lip, "Possible New Sanctions for Uranium," *Korea JoonAng Daily*, November 23, 2010.
[15] Siegfried S. Hecker, "Lessons Learned from the North Korea Nuclear Crisis," *Daedalus.* (2010): 50-54.
[16] Siegfried S. Hecker, "The Risks of North Korea's Nuclear Restart," *Bulletin of the Atomic Scientists* (2009).
[17] Siegfried S. Hecker et al., "North Korea's Choice: Bombs over Electricity," *The Bridge*. Vol. 40, 2 (2010): 9.
[18] Houston G. Wood, Alexander Glaser, and R S. Kemp, "The Gas Centrifuge and Nuclear Weapons Proliferation," *Physics Today (2008)*: 42-43.
[19] Kenneth D. Kok, *Nuclear Engineering Handbook*, Mechanical Engineering Series. (CRC Press 2009), 273-275.
[20] David E. Sanger and William J. Broad, "U.S. Concludes N. Korea Has More Nuclear Sites," *The New York Times,* December 14, 2010.

number of centrifuges has taken on a meaning of its own to signify North Korean nuclear ambitions. Indeed it is typical for an enrichment facility to contain thousands of centrifuges.

One relevant concern regarding the number of centrifuges is how North Korea acquired these parts. Many analysts trace North Korean parts to elaborate procurement schemes through front companies engaged in smuggling.[21] Regardless of whether North Korea's nuclear enrichment parts came from international sources, as analysts suspect, or were developed indigenously, as stated by North Korean officials, extensive UN Security Council sanctions have not prevented North Korea's ability to develop its uranium enrichment program.

Uranium Hexafluoride: A Possible Clue

The number of North Korea's gas centrifuges has received the vast amount of attention, but a more important and less discussed issue is North Korea's ability to produce uranium hexafluoride, a feed material for its gas centrifuges during uranium enrichment.

According to Hecker, "Yongbyon had never admitted having made uranium hexafluoride previously because it is not required for gas-graphite reactor fuel. Yet, now they claim they have this capability on site; however I was not allowed to see it. Nevertheless, my hosts made the case that they have everything they need to run the centrifuge facility."[22]

Even if North Korea could produce Uranium hexafluoride, understanding the purity of the hexafluoride produced is critical to understanding North Korea's ability to feed large scale enrichment facilities. Uranium hexafluoride that fails to meet the purity requirements will corrode the barriers, the separating elements, of the gas centrifuges.[23] If North Korea is achieving less-than-ideal purity for its Uranium hexafluoride, then the current nuclear enrichment facilities would require extensive equipment maintenance and repair to the centrifuges making it costly to run large scale enrichment facilities and seem to contradict some previous claims of North Korea's proliferation activities. If North Korea is adept at producing uranium hexafluoride of optimal purity, it could give credence to the assessment that North Korea was seeking to supply Libya's nuclear facilities in the early 2000's.[24]

Concerns over North Korea's LWR Construction

Several media sources have voiced concerns that a light water reactor could be an opportunity for North Korea to produce weapons-grade plutonium. Given that light water reactors produce "reactor grade plutonium" rather than "weapons grade plutonium," it is a much less attractive means of obtaining plutonium for nuclear weapons.[25] Thus, it could be possible to produce a plutonium bomb, however spent LWR fuel is several steps away from this end and weapons grade plutonium could be acquired by North Korea by other more efficient means. As Hecker pointed out, if North Korea's goal was the production of plutonium, this could be achieved much more easily from the 5MWe gas-graphite reactor that is currently on standby.[26] The light water reactors were proposed in the Agreed Framework[27] specifically because they were formulated more towards the production of electricity than for bombs.

Electric Power vs. Nuclear Weapons

Despite the North Korea's statement of its nuclear energy pursuit and Siegfried Hecker's observations confirming this notion, much of the current dialogue has unequivocally focused on the opportunity for the production of fissile materials. After the Agreed framework was signed, the partially constructed 50MWe gas-graphite reactor (geared towards dual-use) and the 200MWe reactor (seemingly designed for electricity production) were dismantled. With the two promised 1,000MWe LWR failing to come into fruition, it is telling that even North Korea's construction of a 25-30MWe LWR is causing alarm over weapons creation.

Currently, Hecker points out, South Korea operates 20 light water reactors which provides nearly 40% of the country's electricity.[28] He also suggests that, in North Korea's case, "giving up the bomb and developing civilian nuclear power could help lift its economy and its people out of poverty."[29] Now that North Koreans could argue they are beginning down this path, U.S. fears have only increased due to the potential for proliferation and hidden facilities.

[21] David Albright and Paul Brannan, "Taking Stock: North Korea's Uranium Enrichment Program." *The Institute for Science and International Security* (2010): 2.

[22] Siegfried S. Hecker, "Redefining denuclearization in North Korea," *Bulletin of the Atomic Scientists*. December 20, 2010.

[23] Kenneth D. Kok, *Nuclear Engineering Handbook*, Mechanical Engineering Series. (CRC Press 2009), 270-271; David Albright and Paul Brannan, "Taking Stock: North Korea's Uranium Enrichment Program." *The Institute for Science and International Security* (2010): 8.

[24] Ibid., 9-10.

[25] U.S. Department of Energy, *Nonproliferation and Arms Control Assessment of Weapons-Usable Fissile Material Storage and Excess Plutonium Disposition Alternatives.* Office of Scientific and Technical Information. Department of Energy. (January 1997): 38.

[26] Siegfried S. Hecker, "A Return Trip to North Korea's Yongbyon Nuclear Complex," *Center for International Security and Cooperation of Stanford University* (2010): 6.

[27] The Agreed Framework was signed in 1994 between the United States and the Democratic People's Republic of Korea (North Korea) whereby North Korea would freeze its nuclear reactors and related facilities in exchange for more efficient nuclear energy technology and steps towards normalization of political and economic relations between the two countries.

[28] Siegfried S. Hecker, Sean C. Lee, and Chaim Braun, "North Korea's Choice: Bombs over Electricity," *The Bridge*. Vol. 40, 2 (2010): 9.

[29] Ibid., 10.

Speculation of Hidden Facilities

The revelation of hidden nuclear facilities in North Korea is a recurring theme in media coverage and in negotiations. Such concerns are legitimate however international actions on such certainties have come at a steep price. Don Oberdorfer, a Korea expert, described how North Korean negotiators in 1999 were able to use American concern over a possible nuclear facility for a nuclear weapons program at Kumchang-ni cavern to obtain 600,000 tons of UN food for access to the facility, which "was not a nuclear facility and was unsuitable for such purposes."[30] Regardless of whether there is agreement on Oberdorfer's interpretation of the Kimchang-ni negotiations, he highlights the risks associated with estimating the size and capabilities of North Korea's nuclear facilities. North Korea's capacity to produce and proliferate nuclear weapons combined with their past demonstration of nuclear tests and possession of weapons grade uranium spawn speculation and alarm over the existence of covert nuclear facilities and the stockpiling of more fissile material. Overestimation of the extent of North Korea's covert nuclear facilities risks providing North Korea with extra negotiating leverage and sending the IAEA and international intelligence analysts on a wild goose chase.

VI. Reactions and Prospects of North Korea and the NPT

Concern over North Korea's ability to proliferate or produce nuclear weapons will always be a primary concern and indeed past missile tests and evidence of proliferation may legitimize these sentiments. It is absolutely essential, however, that our fears do not dictate the facts on which we base negotiations with North Korea. As Hecker describes lessons learned from the North Korean crisis, he observes, "In Washington, the threat was often exaggerated for political purposes. Hence it is important to get accurate, publically available technical assessments of nuclear capabilities."[31]

Currently progress in multi-lateral negotiations are stalled until North Korea takes visible steps to dismantle its nuclear program, relegating direct talks between the U.S. and North Korea to unofficial diplomatic missions.[32] The wide discrepancy over the perceived threats from North Korea regarding its proliferation of nuclear weapons, the possibility of additional enrichment facilities, and the capacity to divert uranium to increase its nuclear stockpile makes it difficult to pin down exactly what the steps towards might denuclearization consist of.

The Limits of future IAEA Oversight and North Korean NPT Membership

The resumption of IAEA inspections is a critical first step but not a solution to "resolving the North Korean nuclear issue." IAEA oversight can verify that North Korea is not converting their enrichment facilities to produce highly enriched uranium or diverting fissile material, however concerns regarding covert facilities, nuclear proliferation, and North Korea's pursuit will likely continue to plague the oversight process, as it has in the past. North Korea is not currently a NPT member state, the country announced its withdrawal 1993 and officially withdrew in 2003. However, even if the country returned to the NPT and accepted the safeguards, concern over dual-use nuclear technology and weapons proliferation will likely remain. Addressing such concerns requires looking beyond the scope of North Korea's nuclear program to address the scope IAEA oversight and the limitations of the NPT. The NPT upholds the "inalienable rights of all parties to the treaty to develop research, production and use of nuclear energy for peaceful purposes... in conformity with Articles I and II of this treaty" (Article IV of the NPT), however, North Korea violated Article II with its production and test of nuclear weapons. Given that North Korea is the only country to withdraw from the NPT, there is question of exactly what rights North Korea has under the NPT for nuclear energy production given previous treaty violations.

If North Korea were to rejoin the NPT, given that they are considered a non-nuclear weapons state, they would be required to submit to the Safeguards Agreement and confront the same issues as in the past. Michael Spies notes the limits of IAEA safeguards application in that "they do not address the circumstances where a state has diverted nuclear material using indigenous material and equipment, as was the case in North Korea."[33] According to Article XII.7 of the IAEA Statute, "In the event of non-compliance... [the Agency can] suspend or terminate assistance and withdraw any materials made available by the Agency or a member." Such actions would be irrelevant to North Korea who claims to use indigenous talent and equipment for their program or is able to acquire the material amidst United Nations Security Council (UNSC) sanctions.

If North Korea agreed to the Additional Protocols INFCIRC/540 this could assuage fears of possible clandestine nuclear facilities in North Korea because it would give the IAEA authority to investigate undeclared locations by carrying out "location-specific 'environmental sampling.'"[34] North Korea would be highly unlikely to approve such a drastic increase in IAEA oversight because the Additional Protocols also provides the IAEA with the right to access and require reporting on all activities throughout the entire nuclear fuel cycle from mining to production (Article 5.a). By requiring

[30] Don Oberdorfer, The Two Koreas. (Basic Books, 2001), 412.
[31] Siegfried S. Hecker, "Lessons Learned from the North Korea Nuclear Crisis," *Daedalus.* (2010): 50-54.
[32] Christopher Weber, "Bill Richardson Travels to North Korea on Unofficial Diplomatic Mission," Politics Daily. December 14, 2010.
[33] Michael Spies, "Iran and the Limits of the Nuclear Non-Proliferation Regime," *American University International Law Review* (2006): 419.
[34] Theodore Hirsch, The IAEA Additional Protocol What It Is and Why It Matters. *The Nonproliferation Review* Fall-Winter (2004): 144

North Korea to enable access to its production capabilities, North Korea would have to prove that it is indeed capable of manufacturing all the components for its nuclear facilities, as they had previously claimed, or risk losing face with evidence that North Korea did indeed import much of their equipment. Any discrepancy over claims of importing or exporting materials or the indigenous production of certain parts will likely invite further increase scrutiny of North Korea's endeavors. Compliance with additional protocols is viewed as a confidence building measure, not required but once signed is legally binding. Due to the increased IAEA scrutiny and the legal risks faced by North Korea rejoining the NPT and submitting to the Additional protocols, extensive and comprehensive IAEA inspections will likely take time to implement, and thus it is critical for the international community to achieve some current oversight through negotiations.

VII. Recommendations

Given the overall negative reception of Pyongyang's showcase of its progress in nuclear endeavors, much of the attention over relations with North Korea has narrowed in on denuclearization. Carlin and Lewis elucidate the key to success in past negotiations: "The negotiations themselves were stuck until the United States recognized the agreement would have to go beyond nonproliferation."[35] With the six-party talks stalled over the U.S. demand for North Korean to take steps towards denuclearization, any resulting negotiation would likely incorporate the sticks and carrots method to try and settle U.S. concerns about North Korea's nuclear threat. As Carlin and Lewis illustrate, this short term approach ignores North Korea's strategic needs. One of the most obvious needs, in light of North Korean claims and efforts, is the provision of energy. A second overall need that Carlin and Lewis describe is a "desire for a long-term, strategic relationship with the United States that."[36]

The inability for UNSC sanctions to prevent the development of North Korea's nuclear development demonstrates that North Korea could continue expanding its nuclear program. If the U.S. would like to influence the outcome of North Korean nuclear initiatives it would seem there is no choice but to engage in negotiations. Hecker proposed one basis for negotiation, in what he calls "the three no's – no more bombs, no better bombs, and no exports – in return for one yes: Washington's willingness to seriously address North Korea's fundamental insecurity along the lines of the joint communiqué."[37]

Given both North Korea's desire to develop its nuclear power infrastructure while ideally developing a long-term strategic relationship with the United States, the United States should respond by trying to play a role within North Korea's nuclear fuel cycle. One possible role could be engaging in a trade whereby the U.S. acquires North Korean spent fuel rods and then provides new fuel rods for North Korean LWR. Simply stated, the U.S. needs to develop a strategic partnership with North Korea in a manner that accommodates North Korea's efforts to achieve energy security, while providing acceptable oversight and control over opportunities for diversion of fissile material.

In the 1997 KEDO[38] reached a procurement agreement, in which it was to provide LWR fuel. This agreement obviated the need to develop uranium enrichment facilities in the DPRK and it contributed toward an easing of fears regarding the production of fissile material from uranium enrichment. If the Agreed Framework had gone through, under Article III.2 of the NPT, the provision of nuclear fuel would have enabled safeguard protocols and IAEA oversight of the proposed LWR even with North Korea's non-member NPT. Now that North Korea has demonstrated its commitment and ability to develop uranium enrichment facilities the United States must find a way to establish the oversight that is desperately needed.

Although U.S. acquisition of North Korean spent fuel rods is oriented towards back-end reprocessing as opposed to the KEDO agreement of front end orientation, both proposals represent an attempt to assuage fears about potential "cheating" by engaging in long-term partnerships. Now that North Korea is no longer part of the NPT, the U.S. should be trying to gain some insight into North Korean nuclear activity by becoming integrated into North Korea's nuclear cycle rather than further isolating North Korea.

[35] Robert Carlin and John W. Lewis, "Negotiating with North Korea: 1992-2007," Center for International Security and Cooperation of Stanford University. January (2008): 5.

[36] Robert Carlin and John W. Lewis, "Negotiating with North Korea: 1992-2007," Center for International Security and Cooperation of Stanford University. January (2008): 21.

[37] Siegfried S Hecker, "What I Found in North Korea," *Foreign Affairs*. December 9, 2010.

[38] KEDO is a consortium of countries including the United States, Japan, and South Korea developed in 1995 to provide funding and assistance for the implementation of the key parts of the Agreed Framework. Its responsibilities included the financing of the two Light Water Reactors.

Cross-Spectrum Similarities Between Violent Non-State Actors

Sean Atkins

Introduction

Understanding armed non-state organizations is one of the most pressing concerns in today's security environment. Whether on the local, state, or international level, violent non-state actors as a whole represent one of the most troubling issues for national security practitioners, and the danger they pose is compounded by their nebulous and elusive natures. As John Robb, a theorist on the evolution of warfare and former special operations pilot, described in his testimony before the US Congress last year:

> The threat the US faces today is as dire as the darkest days of the Cold War. In fact, this threat may be even more dangerous because it is so insidious. The threat we face is a combination of global systemic threats … and the rapid emergence of violent non-state groups ...[1]

It is also a problem that continues to grow in scope. Terror, insurgent, militia, and criminal groups, equipped with readily available communication and travel technology, have shifted from regional to major strategic challenges. They have increased their "organizational effectiveness, their lethality, and their ability to operate on a truly worldwide scale."[2]

Further complicating the matter, contemporary researchers have recognized a growing nexus between various types of groups (whether analyzing insurgent groups in Iraq, terrorist groups like Al Qaeda or street in gangs in South America) and increasing similarities in how they operate. These similarities and their increased threat potential urges us to examine the follow-on questions: do deeper similarities exist between these groups and, if so, can the way we deal with one set of groups provide any lessons in dealing with another?

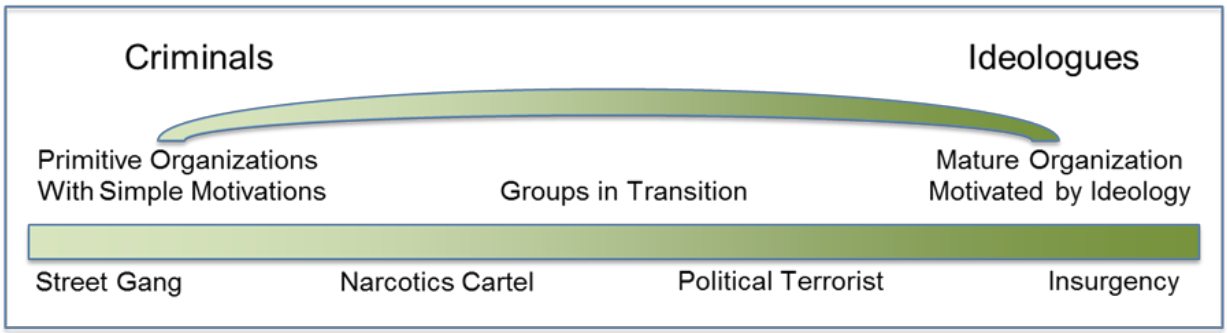
Overview

This article explores the possibility of deeper similarities between armed non-state groups. It attempts to move beyond top layer similarities (such as in methods, stated motivations or goals - all of which have been addressed elsewhere) and to discern similarities in more fundamental variables and characteristics in order to answer the question: What fundamental similarities exist between violent non-state actors? In the end it proposes that, while there are no universal variables or characteristics, many are exceedingly common.

The following analysis utilizes extensive research within one category of violent non-state actor, street gangs, and compares this to primary and secondary evidence regarding other violent non-state actors. Instead of searching for similarities in what they do, it investigates the likenesses in variables and characteristics at the individual, group and community levels. Most of this evidence is relatively recent and therefore primarily qualitative. There are, however, sections that utilize quantitative data where it is available.

The VNSA Continuum[1]

For purposes of this paper the continuum belowwas developed and will be referred to in the sections ahead:



[1] Robb, John. Congressional Testimony. House Armed Services Committee. 2 Apr 2009.

[2] Hanlon, Querine H. "Globalization and the Transformation of Armed Groups." Armed Groups: Studies in National Security, Counterterrorism, and Counterinsurgency. Ed. Jeffrey H. Norwitz. Washington D.C. US Department of the Navy. 2008.

The Continuum

Traditionally, armed non-state groups have been distributed along a horizontal continuum. They are generally grouped by logical distinctions in:

1. Motivation[3]
2. Size
3. Organization
4. Function

Blurring of Lines

In more recent years international security researchers have noticed a blurring of the lines traditionally observed between VNSAs across the continuum. This blurring has been evident in motivation, size, organization and particularly function. What this may imply is deeper commonalities between these groups than had been considered before.

Observers are now finding that many distinctions previously made between VNSAs are "no longer very useful for discerning or assessing the security landscape."[4] Oehme describes the situation as thus:

> …terrorists and insurgents are resorting to organized crime … also opportunistically seeking out criminal networks when specialized support is needed... Conversely, violent criminal organizations have been known to employ operational approaches similar to terror networks to intimidate or gain concessions from provincial government officials…[5]

Groups that take one particular form are found assuming the functions of others such as insurgent groups robbing banks or criminal groups defending minority populations at risk.[6] For instance, IRA activities today primarily consist of local intimidation for economic or political purposes as well as the occasional spectacular bank robbery.[7] Political insurgents in Iraq frequently resort to kidnapping, embezzlement, oil smuggling, theft, fraud and extortion.[8] In the Philippines the Abu Sayyaf Group, a terrorist organizations in the southern islands, has conducted kidnappings, bank robberies and general looting activities.[9] As insurgencies have urbanized away from rural bases they have come to share a similar environment to urban criminal groups like street gangs. This environmental shift may be one reason for adapting techniques and operational methods.[10]

Blurring is not limited to insurgent or terrorist groups. Similar conclusions are being drawn about criminal organizations like gangs. As Max Manwaring, an expert in insurgencies and their relation to gangs, recognized:

> whether a gang is specifically a criminal or insurgent type organization is irrelevant. Its putative objective is to neutralize, control, or depose governments to ensure self-determined (nondemocratic) ends.[11]

Examples of this abound. Recently drug cartels in Juarez, Mexico, have been able to wrest control from the government. In one case the a cartel was able to remove the police chief, Roberto Orduña Cruz, by vowing to kill a police officer every 48 hours until he resigned.[12] They have also intimidated the mayor himself, threatening to decapitate him and his family unless he backed off.[13] Gangs and other criminal groups are challenging the "legitimacy of the state, particularly in regions where the culture of democracy is challenged by corruption and reinforced by the inability of political systems to function well enough to provide public goods."[14] They are acting as surrogates or alternative governments in these areas as well as infiltrating governmental and nongovernmental organizations to further their aims.[15]

Youth Aspect

A benefit of comparing gang studies to information regarding other VNSAs is their focus on the youth component. Studies have determined that gang-joining rates vary by age with the highest levels found in the teenage years.[16] This can be useful as the analysis drawn from here may be well suited to address the youth component of other VNSAs.

Youth involvement in VNSAs across the spectrum is often recognized as a critical component but is not always addressed or understood. Within most VNSAs it is usually the youthful component, at the bottom of the organization, that makes up the mass of its ranks and are most often the ones conducting the majority of the group's operations. This is illustrated by the vertical spectrum overlaid on the horizontal VNSA continuum.

---

[3] Underwood, Peter T. "Pirates, Vikings, and Teutonic Knights." Armed Groups: Studies in National Security, Counterterrorism, and Counterinsurgency. Ed. Jeffrey H. Norwitz. Washington D.C. US Department of the Navy. 2008.

[4] Oehme, Chester G. III. *Terrorists, Insurgents, and Crime – Growing Nexus?* Studies in Conflict and Terrorism. 31:1, 80-93. 2008.

[5] Ibid.

[6] Hoyt, Timothy D. "Adapting to a Changing Environment: The Irish Republican Army as an Armed Group." Armed Groups: Studies in National Security, Counterterrorism, and Counterinsurgency. Ed. Jeffrey H. Norwitz. Washington D.C. US Department of the Navy. 2008.

[7] Ibid., 55

[8] Oehme, 85

[9] Frake, Charles O. "Abu Sayyaf: Displays of Violence and the Proliferation of Contested Identities Among Philippine Muslims." American Anthropologist 100.1 (1998): 41-54.

[10] Hoffman, Frank G. "Neo-Classical Insurgency?" Parameters. Summer, 2007: 71-87.

[11] Manwaring, Max G. A Contemporary Challenge to State Sovereignty Gangs and Other Illicit Transnational Criminal Organizations in Central America, El Salvador, Mexico, Jamaica and Brazil. Carlisle: Strategic Studies Institute. 2007.

[12] Lacey, Marc. "With Force, Mexican Drug Cartels Get Their Way." New York Times. 01 March 2009. Accessed 8 Mar 2009. (http://www.nytimes.com/2009/03/01/world/americas/01juarez.html?em)

[13] Ibid.

[14] Manwaring, 10

[15] Ibid.

[16] Klein, Malcom W. and Maxson, Cheryl L. Street Gang Patterns and Policies. Oxford. Oxford University Press. 2006.

Age Spectrum Overlaid the VNSA Continuum

This point is evident in Afghanistan where youth play a visibly large role within terror and insurgent groups. Indeed, the very first US military member killed in the war on terror "was a Green Beret killed by a 14-year-old sniper."[17] On the release of a video showing a boy beheading a blindfolded man, Taliban commander Mullah Hayatullah Khan commented, "...We want to tell the non-Muslims that our youngsters are… Mujahadeens and… will be our Holy War commanders in the future."[18] Even Senior Al Qaeda leader Ayman Al-Zawahiri first became an active member of a Jihadi cell at the age of 16.

In Iraq, with its myriad of active VNSA groups, youth also play a central role. Even in 2004, very early on, there were 107 juveniles classified as high-risk security threats held in the Abu Ghraib prison alone.[19] By 2007 some 800 juveniles, between the age of 11 and 16, were held in detainment facilities.[20] Foreign fighters flowing into Iraq were mainly young men.[21] As Zaki Chehab, a journalist who interviewed insurgents inside the Iraq resistance, recognized, "...Hundreds of disaffected young Arabs from every kind of background, whether Islamists or nationalists… wasted no time in volunteering."[22] He further noted that although weapons were available to all and most Iraqis had training, "those who actually carried out the attacks were young Islamists."[23] In traveling through Iraq, interviewing the insurgents Ghaith Abdul-ahad found that they all "dreamt of being part of the jihadi movement, of being mujahedeen … all those people are young – 16, 17, 20, 25, 30 maximum."[24]

The strong youth component is not limited to Islamic terrorism or insurgency movements. It is reflected in groups operating in different locations, populations and times. For example, the Red Brigades, an Italian terror organization that operated primarily during the 1970's, consisted primarily of youth. In one "typical attack, two youths on a motorcycle shot and wounded Giorgio Bohretti, a 53-year-old bank executive."[25] The importance of the youth aspect to VNSAs is difficult to overstate and the existing gang research may provide useful insight, lessons and perspective for those studying VNSAs elsewhere on the continuum.

Local Aspect

Street gang research also tends to focus on the local. While some gangs have more recently become extra-localized –or even globalized- organizations, they have traditionally been both active and prosecuted on the local level. This is an important asset if attempting to transfer lessons to international security challenges like terrorism and insurgencies, which, at their roots, are local issues that require addressing at that level.

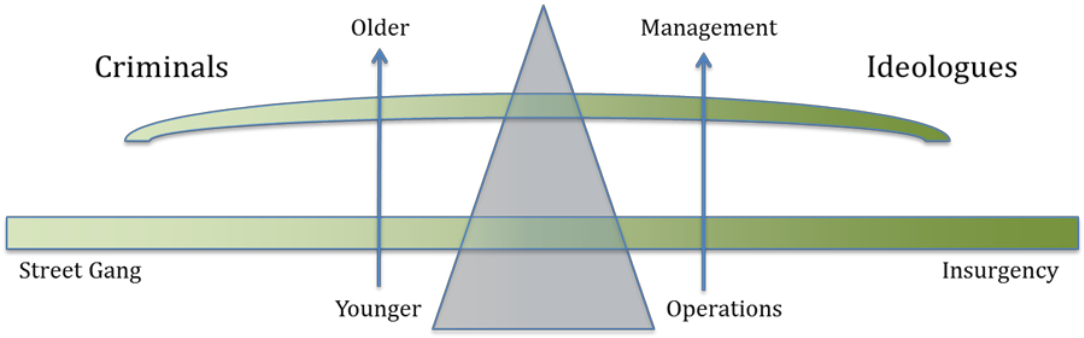
This local focus, even when a group's presence extends beyond a localized area, has recognized benefit when examining other VNSAs. In his testimony regarding the future of VNSAs before the US Congress, John Robb recommended that, "we should focus on the local."[26] He noted that in nearly all of the foreseeable future conflicts involving VNSAs the "ability to manage local conditions is paramount."[27] This is particularly important in today's context where VNSAs, whether operating in a city or across the globe, commonly use decentralized organizational structures that shift autonomy and initiative to local levels.[28]

In analyzing data compiled on the global Jihadi movement, Clint Watts, co-director of PJ Sage, found that city and nodal strategies were far more likely to succeed in disrupting the targeted groups.[29] He suggests:

> ... microscopically focusing on flashpoint cities and dense social network hubs rather than nations or regions … Western countries must look past international boundaries and focus on cities and hubs of radicalization.[30]

Looking at the decades of available gang research, with a long history of focusing on the local, may offer new perspectives and tools with which to approach other VNSAs.

[17] Singer, Peter W. "Children on the Battlefield: The Breakdown of Moral Norms." Armed Groups: Studies in National Security, Counterterrorism, and Counterinsurgency. Ed. Jeffrey H. Norwitz. Washington D.C. US Department of the Navy. 2008.
[18] Reuters, "Taliban video of boy executioner causes anger." 26 April, 2007.
[19] Singer, 362
[20] Ibid.
[21] Felter, Joseph and Fishman, Brian. Al-Qa'ida's Foreign Fighters in Iraq: A First Look at the Sinjar Records. New York. Combating Terrorism Center. 2008.
[22] Chehab, Zaki. Inside the Resistance. New York. Nation Books. 2006.
[23] Ibid., 18
[24] Abdul-ahad, Ghaith. Interview. Frontline. Public Broadcasting Corporation. Aug 2005. Accessed 21 Jan 2009. (http://www.pbs.org/wgbh/pages/frontline/insurgency/interviews/abdulahad.html)
[25] Smith, Paul J. "The Italian Red Brigades (1969-1984): Political Revolution and Threats to the State." Armed Groups: Studies in National Security, Counterterrorism, and Counterinsurgency. Ed. Jeffrey H. Norwitz. Washington D.C. US Department of the Navy. 2008
[26] Robb
[27] Ibid.
[28] Hanlon, 119
[29] Watts, Clint. Beyond Iraq & Afghanistan: What Foreign Fighter Data Reveals About the Future of Terrorism. PJ Sage. 2008
[30] Ibid., 6



Age Spectrum Overlaid the VNSA Continuum

Commonalities

This section addresses common fundamental variables, risk factors and characteristics between gangs and other VNSAs. It is divided into three sections, each addressing a different level of analysis: individual, group and community.

The first thing to note is that it moves beyond simple explanations of stated grievances to find common underlying factors. In examining 1,043 civil-war ex-combatants, Macartan Humphrys, a Columbia University professor and expert in civil war, found that "empirical results challenge standard interpretations of grievance-based accounts of participation."[1] While a group's stated grievances can tell an analyst much, in forming policy decisions there may be utility in looking beyond these.

The second item to note of is that these variables make a complex web of influence. They vary in appearance across different cases. Due to contextual differences, such as culture and location, some are found in a majority of cases studied while others may show up in only a few. Further, these variables often interact with each other increasing their overall influence.

Individual Level Factors

At their lowest level terror attacks and insurgent operations are a matter of individual choice. Each terrorist or insurgent chooses to join the group and ultimately to pull the trigger or detonate an Improvised Explosive Device (IED). As anthropologist Charles Frake states, "Current violence, in the mountains of Bosnia, the streets of New York, the pubs of Belfast, the subways of Tokyo, and the islands of the Philippines, is, in the situation and moment of occurrence, an act of individuals with individual motives and intent."[2] What follows is an analysis of some of the factors that influence the motives and intent of those individuals who choose to participate in violent non-state groups.

Previous Criminal Acts

It may be obvious, but nonetheless useful, to note that prior illegal activity may identify those who are more susceptible to recruitment into what are essentially criminal organizations, whether a street gang, insurgent or terrorist group. A study on gangs produced for the Canadian government summarizes a vast collection of gang studies when stating that, "researchers have indicated that prior acts of delinquency were significantly correlated with a youth's decision to join a gang."[3]

Past illegal activity indicates an attitude or outlook that finds it less difficult to cross legal or moral boundaries. A majority of gang studies that focus on individual variables "find that 'youth attitudes toward delinquent behavior' is a risk factor.[4] A clear terrorist or insurgent example of this factor was Abu Musab al-Zarqawi, the former leader of al-Qaedai's Iraq-based insurgent organization. He was first arrested and jailed not for bombings or kidnappings, but for petty crimes as a youth in Jordan.[5]

This lack of moral or legal boundaries may also partially explain how some VNSAs can easily move between criminal acts like robbery and kidnapping for ransom to political violence like terror or insurgent attacks. As described in the introduction, VNSAs are sliding back and forth on the horizontal spectrum and often fitting into more than one category simultaneously. If individuals are able to cross moral and legal boundaries for one particular reason then perhaps it is easier to cross them for others, political or otherwise.

Exposure to Turmoil

An individual's exposure to traumatic events, particularly where violence is involved, also appears to be a somewhat common factor shared by VNSAs across

1. [1] Humphreys, Macartan and Weinstein, Jeremy M. "Who Fights? The Determinants of Participation in Civil War." The American Journal of Political Science 52.2 (2008): 436-455.

[2] Frake, 41

[3] Lafontaine, Tania; Ferguson, Myles and Wormith J. Stephen. Street Gangs: A review of the Empirical Literature on Community and Corrections-Based Prevention, Intervention and Suppression Strategies. Paper prepared for the Canadian Government. June 2005.

[4] Klein, 148

[5] Chehab, 49

the spectrum. Locations where much of VNSA activity is concentrated provide countless violent situations to influence potential recruits. Personal experiences with extreme violence, whether in South Central Los Angeles, Palestine or Iraq can influence individuals' life choices and provide justification for and normalization of violent activities.

Gang and terror group studies appear to agree on this point, many of which note that those who were exposed to violence and emotional distress in their childhood were more likely to become involved.[6] Klein and Maxson noted that, generally speaking, there were a higher concentration of youth who experienced a series of negative life events in gangs.[7] Kellerhals, in researching terrorist groups, found that:

> Individuals who endure trauma may undergo *dissociation*, or a state of already being dead. This type of mental freezing… can lead the individual to become unemotional about killing another human being. Those generations who see or experience war, torture and other horrors eventually normalize violent acts in their minds... These people find it much easier to become a terrorist or a suicide bomber.[8]

Identity

Seeking to build or find one's identity is a common and strong factor for those joining VNSAs. This is particularly true for younger individuals and for those who feel detached from their ethnic, cultural or other bases for identity. The Canadian gang study notes that "gang members tended to be persons with identity problems".[9] Specifically cited in multiple gang studies were those who felt weak attachments to their ethnic group or a lack of cultural identity.[10]

Similar to gang membership, issues of identity are commonly found within membership of other VNSAs. As Jessica Stern, Harvard's noted expert on terrorists and militants, stated in a recent interview, "There's a strong feeling of confused identity."[11] Abubakar Janjalani, the principal founder of the Philippine terrorist organization Abu Sayyef Group (ASG) was himself born into a split Muslim-Christian family. In growing ASG, Janjalani "tapped into a large pool of disaffected Muslims… torn from their ethnic roots during the preceding decades."[12] As Juergensmeyer found in researching terror groups, "to live in a state of war is to live in a world in which individuals know who they are, why they have suffered, by whose hand they have been humiliated…"[13]

Defining or redefining individual identity is not always an issue of ethnicity or religious background. The Red Brigades would test potential recruits to ensure they were capable of shedding their old identities and any connection to it, family, friends or otherwise.[14]

Further, for some VNSA members, the motivating force behind the issue of identity may be simpler than a complex detachment from ethnic of cultural roots. While researching The Real IRA and The Continuity IRA, Morton Cole, a UK based journalist, found that many of the youth involved with the resurgence of violence during 2009 wanted to "identify with something that is rebellious."[15] Fahmi Salem Said Al Sani, a Yemeni who travelled to the Al Farouq Al Qaeda training camp in Afghanistan during 2001, remarked that he didn't go to "fight anyone" but because he "felt it was important in coming of age."[16]

The motivation behind an individual's issues of identity may be tied to weak ethnic or cultural foundations, or to something as simple as the urge of youth toward rebelliousness and proving maturity. Either way, an individual's sense of identity and how a group may build or shape that are crucial to youth development and can play a significant role in motivating membership in VNSAs.[17] At the simplest level, VNSA activity is based on individuals seeking to satisfy questions of identity, status, need for belonging, and perceived protection, and not to commit crimes.[18]

Security

Some individuals are drawn to membership in armed groups for the perception of security that it can provide. Among the many individual factors identified in gang research, "safety and protection" often reaches the top of the list.[19] One study that engaged St Louis gangs, for example, showed that members selected protection more often (54%) than any other reason for joining.[20] Follow-up questions from other studies revealed that gang members often felt threatened and joined to seek physical protection, find safety and to protect their neighborhoods.[21]

The logical question that follows identifying "the need for protection" as a factor is: protection from what? The answer to this question can be the same for insurgent and gang member: protection from rival groups. Rival street gang violence is responsible for

---

[6] Lafontaine, 31
[7] Klein, 148
[8] Kellerhals, Merie D. Jr. "Profile of a Suicide Terrorist Defies Common Stereotypes." Americe.gov
[9] Lafontaine, 31
[10] Ibid., 31 and 34
[11] Stern, Jessica. Panel discussant. "The Making of a Terrorist." Talk of the Nation. Hosted by Neal Conan. 18 Jul 2005.
[12] Frake, 48
[13] Meilahn, Kathleen. "The Strategic Landscape: Avoiding Future Generations of Violent Extremists." Strategic Insights. July 2008.
[14] Smith, 18
[15] Cole, Morton. "Real IRA, Real Life." The Independent Mar. 2009. Accessed 16 Apr. 2009. (http://www.independent.co.uk/news/uk/home-news/real-ira-real-life-1645360.html)
[16] Wittes, Benjamin. The Current Detainee Population of Guantanamo: An Empirical Study. Washington D.C. Brookings Institution. 2008. Accessed 04 Jan 2009. (http://www.brookings.edu/~/media/Files/rc/reports/2008/1216_detainees_wittes/1216_detainees_wittes.pdf)
[17] Maggio, Edward J. "The Threat of Armed Street Gangs in America." Armed Groups: Studies in National Security, Counterterrorism, and Counterinsurgency. Ed. Jeffrey H. Norwitz. Washington D.C. US Department of the Navy. 2008.
[18] Klein, 8
[19] Lafontaine, 31
[20] Klein, 157
[21] Ibid.

hundreds of deaths in the US annually. In Los Angeles in 1987, for instance, members of gangs were held responsible for 205 deaths.[22]

This targeting of "enemy" individuals and communities, and the insecurity it produces, is often mirrored in civil war or insurgent situations. On a far larger scale, nearly 1,400 Iraqi civilians were murdered in targeted killings in Baghdad during May of 2006.[23] Sectarian based violence has torn apart much of Iraq and produced innumerable localized insurgent groups. In addition to fighting the coalition, these groups are set up to defend against targeted sectarian attacks. Reactionary groups "often form in response to threats to their communities … focus on the traditional military task of protecting the population."[24]

Iraq is a stark example but not the only one. In Sierra Leone VNSAs vying for power fueled a particularly bloody conflict. Fighters within civil-warring groups generally believe that they are safer inside a fighting faction than outside of it.[25] Humphreys, who has researched this angle of the conflict extensively, found that:

> The relationship between personal security and the decision to join a rebellion is strongly significant … even after controlling for a range of other factors …The possibility of improving one's personal security, it appears, provides an important motivation for joining a faction ...[26]

VNSAs persist because they satisfy particular needs of their members. Among the more prominent is the perceived protection membership provides from rival groups.[27]

Free Time

VNSA members often possess excess leisure time and have few meaningful activities to occupy it with. The previously mentioned Canadian study noticed that research often found that gang members reported a greater amount of unstructured time spent with their peers.[28] Several gang studies go on to identify seeking "excitement" as a reason for membership.[29] Membership offers gratification to individuals with a need for engaging activities and who possess excess free time.

This factor also appears in detainee data from Guantanamo and records on foreign fighters captured from insurgents in Iraq. The modern Sunni mujahid who volunteers to fight as a terrorist or insurgent "has time on his hands and a lack of purpose, making him more susceptible to radicalization and giving him enough free time to travel in support of jihad."[30] Tales of "Jihadi adventure" in foreign lands from returning fighters can be influential to youth under the influence of this factor. In interviews with Jared Cohen, young Palestinian militants commented, "What choice do we have? They try to create special programs for us to experience life outside the camps, but we still face so many problems… we have no entertainment."[31] This lack of meaningful activity or purpose, in particular, links directly into the next common factor between VNSA members: desire for a purpose in life.

Purpose Seeking

Gang and insurgent/terror group members share the desire for a purpose to their lives that membership in these groups appears to offer. Gang research describes the typical gang member as someone who had lower feelings of purpose in life.[32] Whereas the typical gang member might find purpose in protecting his neighborhood, modern Jihadis are commonly influenced by the idea of "devotion to his faith and community.[33]

Ghaith Abdul-Ahad, an Iraqi reporter who has interviewed countless insurgents, recounts his conversation with a group of foreign fighters in Northern Iraq:

> They dreamt of being part of the jihadi movement, of being mujahideen, and Iraq provided them with the opportunity to fulfill this dream, ...to send people, send money, create the ideological cause… But for those young men, ... they have this romantic dream of Osama bin Laden, of mujahideen, of Afghanistan, and they wanted to fulfill these dreams in Fallujah and Iraq.[34]

Jared Cohen found similar desires and dreams in his discussions with young Lebanese Fatah militants. One of the groups he spoke with commented that, "inside here we are somebody… We want to contribute to society… At least if we fight, we feel as though we belong to something that is trying to bring about change.[35]

It is not only Jihadis and gangsters that are motivated by a need for purpose in life. The Italian Red Brigades provide another example. The Red Brigades was originally commanded by Renato Curcio and his wife Margherita Cagol, who were trained hotel bookkeepers that found their mundane lives unappealing.[36] They found greater purpose in creating a movement to

---

[22] Reinhold, Robert. "Gang Violence Shocks Los Angeles." New York Times. 08 Feb 2008. Accessed 04 Jan 2009. (http://www.nytimes.com/1988/02/08/us/gang-violence-shocks-los-angeles.html)

[23] Borger, Julian and Howard, Michael. "Baghdad has Bloodiest Month as 1,400 targeted Killings Add to Toll." The Gaurdian Jun. 2006. Accessed 20 Apr. 2009. (http://www.guardian.co.uk/world/2006/jun/07/iraq.iraqtimeline)

[24] Hammes, T. X. "Armed Groups: Changing the Rules." Armed Groups: Studies in National Security, Counterterrorism, and Counterinsurgency. Ed. Jeffrey H. Norwitz. Washington D.C. US Department of the Navy. 2008.

[25] Humphreys, 442

[26] Ibid., 449

[27] Klein, 165

[28] Lafontaine, 30

[29] Ibid., 34

[30] Watts, 2

[31] Cohen, Jared. Children of Jihad. New York. Gotham. 2008.

[32] Lafontaine, 31

[33] Watts, 8

[34] Abdul-Ahad

[35] Cohen, 172

[36] Smith, 16

facilitate the social and political changes that they believed were inevitable.[37]

Status, Respect and Power

Youth are often motivated by the idea of wielding power over others and earning respect and status within their social group. One of life's major motivators "on occasion not even second to survival, is the need to be somebody."[38] Studies have consistently identified "status and respect" as the top reason for gang membership.[39] Additionally, Gordon found that "status deprivation can be a cause of delinquency.[40]

A similar desire for power, status and respect may influence insurgent and terrorist group recruits as well. In researching ASG in the Philippines, Frake found that the need to be "somebody" was only satisfied through recognition from one's fellows.[41] Writing on Abu Musab al-Zarqawi, Mary Anne Weaver, a noted journalist who has covered militant Islam extensively, remarked that there was "a cachet involved in fighting the jihad."[42] After fighting in Afghanistan, Zarqawi discovered that the community that had previously ignored him had now accorded him a high social position and respect. As with many VNSA members, maintaining and increasing social position became an important motivating factor for Zarqawi's future activities. To help understand this, Singer asks us to:

> Imagine the temptation you might have if a group of older boys wearing natty uniforms and cool sunglasses were to show up at your school and force all the teachers to bow down to show who is "really in charge." They then invite you to join them, with the promise that you too can wield such influence.[43]

Family and Peer Factors

In addition to the individual's search for private meaning and social respect, there is the semi-public influence of one's family and friends. Modern gang literature reveals that peer and family-related factors are highly influential in gang participation and a weak family foundation is a significant indicator of participation.[44] Gordon found that "within delinquents' families, marital relations were poorer, there was less family cohesion, less affection shown… by both parents."[45] As a result, the sons felt weaker emotional ties to their parents and had a lower estimate of his parents' concern for their welfare.[46]

Although the evidence is not as plentiful as in gang research, weak family systems do appear to be a factor for membership to insurgent or terror groups. A group of more than 200 Saudi sociologists, who gathered in Riyadh in 2005 to discuss terrorism, concluded that "an unhappy home is the cause of youths going astray and eventually taking to terrorist activities."[47] One of the sociologists pointed out that broken homes are bereft of understanding or communication and that "such a family environment leads to frustration, which eventually leads the youth to be misfits in society who resort to nefarious activities."[48]

It is not only lack of family involvement that encourages VNSA membership; families and friends can also actively encourage membership through their own affiliations. Family or peer connections to gangs can provide the quick track to membership, which is reflected in the findings of multiple gang studies and in the experience of insurgents/terrorists.[49]

A 2003 study of Rochester gang members found that more than half indicated that having friends or family in the gang was the *primary* reason they joined.[50] Studies conducted by Howell and Lahey found that previous association with antisocial peers was a significant contributor to gang membership.[51] Klein, with further analysis on this variable, notes that friend relations is not only a risk factor for gang joining, but they can influence of amplify other risk factors as well.[52]

For potential terrorists or insurgents family members and friends provide the social pressure and reinforcement of political or religious justifications for violence.[53] Analysis of the Sinjar Records, a foreign-insurgent registry in Iraq, shows that friendships played a key role in recruitment.[54] Many of the fighters crossed into Iraq with hometown friends, suggesting that al-Qaida targeted existing groups of friends.[55] Interviews with Guantanamo detainees suggests a similar pattern for terrorists and insurgents captured in Afghanistan. The data indicates that returning fighters influenced groups of friends to join them and that the ones that did so travelled together, presumably reinforcing each other's decision.[56]

Group Level Structure and Processes Factors

Studying VNSAs at the group level explains the rationale for their operational motivations and

[37] Ibid., 17
[38] Frake, 41
[39] Lafontaine, 34
[40] Gordon, Robert A. "Social Level, Social Disability, and Gang Interaction." The American Journal of Sociology 73.1 (1967): 42-62.
[41] Frake, 41
[42] Weaver, Mary Anne. "The Short, Violent Life of Abu Musab al-Zarqawi." The Atlantic. Jul 2006. Accessed 22 Feb 2009. (http://www.theatlantic.com/doc/200607/zarqawi/2)
[43] Singer, 363
[44] Klein, 148
[45] Gordon, 50
[46] Ibid.
[47] Rasooldeen, Mohammed. "Broken Homes Blamed for Turning Youth to Terrorism." Arab News. 24 Mar 2005. Accessed 13 Dec 2008. (http://www.arabnews.com/services/print/print.asp?artid=60962&d=24…Broken%20Homes%20Blamed%20for%20Turning%20Youth%20to%20Terrorism)
[48] Ibid.
[49] Lafontaine, 34
[50] Klein, 157
[51] Lafontaine, 30
[52] Klein, 147
[53] Watts, 8
[54] Felter
[55] Ibid., 28
[56] Watts, 2

procedures and can also expose opportunities for effective counter-VNSA strategies.

Image, Media and Recruitment

A VNSA's image is paramount to its continued existence and growth. It is the group's image that addresses and exploits the individual's psychological needs: status, respect, power, identity, purpose and perception of security. The image is often communicated via readily accessible mass media such as the internet, music, or television or even by word of mouth from local veterans.

Image building and recognition are essential to the recruiting process. Gang imagery distributed through the popular media (movies, clothing styles, music, …) "seems to have more influence on local gang activity" than movement of actual gang members.[57] Once spread into the popular youth culture, containment of a gang's image has proven difficult. Even the Saudi Arabian government could not prevent Sunni-led Islamic militant groups from crossing into Iraq once the movement was popularized among Saudi youth.[58]

The internet is a vital medium in VNSA image campaigns, whether terrorist, insurgent or domestic street gang. Many of America's most notorious gangs have become web-savvy, "showcasing illegal exploits, making threats, and honoring killed and jailed members.[59] This seems a direct parallel to insurgent and terror websites which showcase videos of their violent acts with the logo of the group claiming responsibility, post audio or video clips of threatening speeches by leaders, and honor killed and captured members.[60]

Some particularly marketing-savvy VNSA groups have established "lifestyle" publications that promote the group's activities and interests to aspiring members and the curious public. The January 2009 issue of Sada al-Malahim, an online magazine published by Al-Qaeda in Yemen, contained "a word from sheik Dr. Ayman al-Zawahiri", an article on Al-Tayammum and life in prison, and the story of "The Lion of Jawf: Amir Huraydan" among others.[61] An Urdu language online magazine published by the militant group Jaish-e-Mohammad and targeted for the pre-teen demographic, suggests that militants assume greater social status than doctors or engineers.[62]

Public media attention, even when negative, is also central to building a VNSA's image. Nightly newscasts that detail gang violence often identify groups by name, publicize the group's activity and help create an image of power and legitimacy. Terrorists, gangs and other VNSAs rely on this media amplification to achieve maximum psychological effect and thus affirm the power of the organization. These legitimate newscasts can spread terror among their targets, and affirmation of success among their sympathizers, sources of funding, and potential recruits.[63]

For example, a March 2006 story produced by the Oakland California CBS affiliate told the "inside story" of the Norteno versus Soreno gang wars.[64] The broadcast pushed the previously-localized gangs into community consciousness and caused generalized fear of the escalating violence. The Abu Sayyef Group, a Philippine terrorist organization, received similar publicity during its naissance when the *International Herald Tribune* featured a story on the group. The article was appointed with a "pagewide photo, obviously staged, of prototypic terrorists trying to look grim… while brandishing a threatening variety of weapons."[65] The headline read: "Islamic Rebels Stun Manila with Their Ferocity."[66]

In addition to mass media, both legitimate and propagandist, there is also a word of mouth element to VNSA image building that plays a central role. Although a community might respond as a whole to mass media, individual recruits are influenced by real-life examples of local gang members who have attained social position and can regale an audience with their exploits. The New York chapter of the Bloods street gang exploited this by organizing meet-and-greet mixers between current members and potential recruits.[67] Likewise, both the Sinjar Records and data on the Guantanamo detainees indicate that Al Qaeda deploys veteran fighters to return to their hometowns as recruiters.[68]

Oppositional Culture

Many VNSAs exhibit a group culture based on opposition, whether to official authority, rival VNSA group or some other perceived threat to its ascendancy. This oppositional culture establishes a perceived social purpose, of being part of a society of "us versus them struggling to exist in an unfriendly and unforgiving environment.[69] As sociologist Robert Gordon recognized:

> The group interaction brought about by the demands of an external environment for solutions to instrumental problems promotes positive sentiments between members. From these statements it would follow that if a group lacked a

[57] Klein, 57
[58] Chehab, 182
[59] Glazer, Andrew. "Authorities Say Gangs Using Internet." The Washington Post Jul. 2006. Accessed 12 Dec. 2008. (http://www.washington post.com/wp-dyn/content/article/2006/07/06/AR2006070600886.html)
[60] Chehab, 60
[61] Hegghammer, Thomas. "New Issue of Sada al-Malahim." Jihadica. 2009. Accessed 19 Jan. 2009. (http://www.jihadica.com/new-issue-of-sada-al-malahim)
[62] Siddique, Qandeel. "Child Martyrs." Jihadica. 11 Mar 2009. Accessed 11 Mar 2009. (http://www.jihadica.com/child-martyrs)
[63] Meilahn
[64] Vasquez, Joe "Oakland Murders." CBS 5 Evening News. Mar 2006. Accessed 22 Feb 2009. (http://www.youtube.com/watch?v=IrxR_xOKs4)
[65] Frake, 41
[66] Ibid.
[67] Conte, Michaelangelo. "Weehawken Police Interrupt Suspected Gang Recruitment Meeting and Walk Away with 'Valuable' Notebook." The Jersey Journal Nov. 2008. Accessed 14 Apr. 2009. (http://www.nj.com/hudson/index.ssf/2008/11/wehawken_police_interrupt_susp.html)
[68] Felter, 28; Watts, 2
[69] Maggio, 190

> task, purpose, or mission as a result of not being integrated into a demanding external system … then it would fail to generate a major part of the rewards and sentiments that its members might expect to gain from it.[70]

Street gangs provide access to and legitimization of oppositional attitudes and behaviors.[71] This culture harnesses the individual's resentment of society's institutions such as the police, schools, or discriminatory employers.[72] In his studies of urban street gangs, Venkatesh found a common ideology regarding "the authorities as wholly or partially hostile or as unappreciative of the things which really matter."[73]

The same can be said about other VNSAs across the horizontal spectrum. Insurgent groups are, by their very definition, founded on opposition to existing power structures. Abu Musab al-Zarqawi emphasized his group's oppositional culture by describing the Iraqi government and its security forces as composed of "infidels".[74] The Armed Islamic Group of Algeria (GIA) rejected not just the Algerian government but also much of Algerian society as kuffar (apostates).[75] This opposition can be based on deep historical roots. As Frake notes:

> During the course of southern Philippines history, ethnic, religious, political, modernistic, and religionistic strata of identity formation, together with outlaw outcroppings in each stratum, shape the fault lines of divisiveness along which violent conflict threatens to erupt.[76]

Further, counter-VNSA actions by domestic or international institutions can help build and tighten this cultural foundation. As Lien discovered of Oslo based gangs, "the war on gangs justifies the warring gang."[77] Klein, in his review of gang research in the US observed that "each rejection of the gang merely reinforces its cohesiveness and its dependence upon itself.[78] The US Army's counterinsurgency filed Manual also recognizes this same point about insurgencies.[79]

This oppositional culture factor is often based on an idea of injustice and victimization. VNSA members conceive ideas of compassion, love and sacrifice based on self-perceptions as a victim of society's oppression, racism, inequality or suppression.[80] Gang experts Malcolm Klein and Cheryl Maxson found that the perception of injustice and victimization is necessary in order to justify a gang member's acts of violence or other criminal activity. This sentiment is illustrated in the words of Mohammed Sadiq Khan, recorded before taking part in the 2005 London bombings:

> Your democratically elected governments continuously perpetuate atrocities against my people all over the world, and your support of them makes you directly responsible, just as I am directly responsible for protecting and avenging my Muslim brothers and sisters.[81]

Terror groups like Al Qaeda feed on local or larger community grievances.[82] With this justification a VNSA member's actions can be seen as justified, selfless and heroic and victims can be seen as complicit enemies.[83] As Zarqawi stated about members of Iraq's security forces, "those who cooperate with the Americans are infidels… and they deserve to be killed."[84]

The legitimate media can again provide a buttress for VNSA movements. International broadcast of prisoner abuse at Abu Ghraib, videos of Israeli attacks on Palestinian camps or domestic police abuse support the VNSA's rationale for their image as victim-crusaders against an unjust Establishment. In addition to garnering more recruits, these images may also serve to demoralize the general public in official prosecution of VNSAs.

Amplification of Delinquent Behavior

Exhaustive sociological research on group behaviors indicates the behavior of an individual will alter in a group setting. In the case of VNSAs across the spectrum the group process serves to amplify an individual's propensity to commit acts of violence or delinquency. This is especially well-documented within gang studies.

In his research on normative features of gang violence, Decker found that gang violence is at least partially "an outgrowth of a collective process."[85] The *social facilitation model* suggests that gang members' delinquent profiles are similar to non-gang members in the community before they join, and "it is the gang's group processes… that elevate criminal activity."[86] As Gordon notes in his studies, "such a … process may be capable of involving in serious delinquency boys who suffer from milder degrees of social disability, but in whom severe pathology seems absent.[87]

These processes are at work within other VNSA groups as well. Profiles of terrorists or insurgents often reveal a contrast between pre- and post-membership activities in regard to violence or criminality. Even the most seemingly solitary actors, suicide bombers, do not

[70] Gordon, 58
[71] Klein, 158
[72] Ibid., 206 - 207
[73] Venkatesh, Sudhir Alladi. "The Social Organization of Street Gang Activity in an Urban Ghetto." The American Journal of Sociology. 103.1. 1997: 82-111.
[74] Chehab, 56
[75] Byman, Daniel. "Talking With Insurgents: A Guide for the Perplexed." The Washington Quarterly 32.2 (2009): 125-137.
[76] Frake, 51
[77] Klein, 206 - 207
[78] Ibid.
[79] United States Department of the Army. The US Army/Marine Corps Counterinsurgency Field Manual. Chicago. Chicago University Press. 2007.
[80] Ibid.
[81] Khan, Mohammed Sadiq. Videotaped Speech. 1 September 2003. Accessed 4 Jan. 2009. (http://www.memritv.org/clip/en/0/0/0/0/0/144/835.htm)
[82] Army, 8
[83] Klein, 206 - 207
[84] Chehab, 56
[85] Decker. "Collective and Normative Features of Gang Violence." Justice Quarterly 13.2 (1996): 243-264.
[86] Klein, 75
[87] Gordon, 62

operate alone.[88] Prospective bombers and other potential VNSA members follow kin and friends into their organizations.[89] These organizations provide emotional encouragement, financial and religious incentive and logistical support to suicide bombers at every step from their induction into the VNSA to their ultimate act. It is by nature a group activity aimed to amplify an individual's ability to commit acts they would have otherwise avoided.

Studies on gang violence amplification reveal even more about the process and its effectiveness. One controlled study of violence amplification in Rochester gangs, showed that "group-induced crime amplification took place at high rates regardless of the character of the gang neighborhood."[90] This might explain similar observations of the amplification factor within other VNSAs with diverse membership and locales. Further, this amplification appears to be self-reinforcing. With increased criminal activity comes a corresponding boost in group cohesion which itself leads to greater crime involvement and increased resistance to official efforts.[91]

Structure and Leadership

VNSAs across the spectrum are often characterized by loose leadership and decentralized organization. The majority of VNSAs, whether street gang, terror or insurgent group are composed of small loosely-affiliated and semi-autonomous cells. Although there are notable exceptions in groups that maintain greater cohesion and clear hierarchy, this, particularly with contemporary VNSAs, is a smaller fraction.

Street gangs do not generally fit a standard rigid hierarchy. Decker, in his study on collective and normative features of gang violence, found that violence and particularly retaliatory violence was an outgrowth that reflected a loose organizational structure and diffuse goals.[92] Klein and Maxson found while compiling gang research, that street gangs are almost always "more a loose collection of cliques or networks than a single, coherent whole."[93]

Insurgent groups also defy traditional organization and classification.[94] In Afghanistan, for instance, the insurgency is made up of Taliban members, Hezb-i-Islami, the Jalaluddin Haqqani network, as well as local tribes and criminal networks.[95] Each of these groups breaks further down into loosely connected subgroups and clans. Although the diffuse nature allows widespread geographical and social influence, it also subjects VNSAs to the inefficiencies of divergent internal factions and aims.[96]

In Iraq, organizations like Hamas, Salah ad-Din and 20th Revolutionary Brigades have active groups in multiple cities. Zaka Al-Din Abd Al Fatah Suliman, an insurgent tasked with beheading Iraqi national guardsmen, for instance, claimed to be part of a small group headed by Ahmad Ibrahim, which was in turn affiliated with the "Liberation Army".[97] These groups can be classified as affiliates rather than a single cohesive organization. By sharing a popularized brand name, all diffuse activities can be credited to affiliates, increasing their prestige as a whole and attracting publicity and financial support. This does not, however, guarantee uniformity in agenda as various affiliates struggle for ascendency within the larger VNSA. As Curry states, "today's small wars are a 'fur ball' of enabled groups vying for influence."[98]

This amorphous organizational structure is reflected in a loose form of leadership for most VNSAs. For gangs, leadership is generally ephemeral and turnover is high.[99] Group actions are determined more by the group itself and local context than by any particular individual. This is also typical of insurgent groups who must quickly react to and exploit changes in the local social or political contexts. Leadership for modern terror groups reflect this as well where:

> there is no single, central leadership, command, or headquarters … Decision-making and operations are decentralized, allowing for local initiative and autonomy. Thus the design may sometimes appear acephalous (headless), and at other times polycephalous (Hydra-headed).[100]

Community Level Factors

Variables found at the community level are some of the more influential to creation of and participation in VNSAs, and interact heavily with those at the individual and group levels of analysis. As Klein and Maxson found, "the stability of 'ganging' probably lies more in the characteristics of the particular community than in the particular group of young people who comprise the gang."[101]

[88] Hoffman, Bruce. "The Logic of Suicide Terrorism." The Atlantic Jun. 2003. Accessed 10 Sep. 2008. (http://www.theatlantic.com/doc/200306/hoffman)
[89] Kellerhalls
[90] Klein, 163
[91] Ibid., 196
[92] Decker, 263
[93] Klein, 195
[94] Army, 100
[95] Jones, Seth G. Counterinsurgency in Afghanistan. Santa Monica: Rand, 2008.
[96] Curry, Peter E. "Small Wars are Local: Debunking Current Assumptions About Countering Small Armed Groups." Armed Groups: Studies in National Security, Counterterrorism, and Counterinsurgency. Ed. Jeffrey H. Norwitz. Washington D.C. US Department of the Navy. 2008.
[97] Suliman, Zaka Al-Din Abd Al-Fatah. Videotaped Interview. 31 Mar 2005. Accessed 25 Jan 2009. (http://www.memritv.org/clip/en/0/0/0/0/0/144/630.htm)
[98] Curry, 151
[99] Klein, 164
[100] Arquilla, John; Ronfeldt, David; and Zanini, Michele. Networks, Netwar, and Information-Age Terrorism." Countering the New Terrorism. Santa Monica: Rand. 1999.
[101] Klein, 189

Lack of Opportunity

Communities that possess limited or no economic, social or recreational opportunities are particularly susceptible to VNSA development.[102] Lack of employment is a particularly influential variable. Without work potential members have ample free-time (an important individual factor). It also presents an economic motivation to participation in VNSAs. For street gang members the quick and easy income crime provides is attractive. In Iraq, the draw for many insurgents was the promise of pay for each particular act of violence. Further, VNSAs fulfill many social needs such as purpose and status which have been traditionally met by legitimate employment.

Gang research has clearly connected this factor to gang emergence and participation. Klein and Maxson find that gangs are particularly common in areas with "declines in the number of jobs in wholesale, retail, and manufacturing trades." Entry-level positions in these industries typically employ emerging youth.[103] Jackson, Wells and Weisheit's studies on gang emergence highlight economic transitions and disadvantage.[104] Maggio also found that:

> Regardless of race, gangs thrive when certain conditions in a community are present. An area of the nation with continuous poverty, …and decreased social opportunities …can raise the potential for street gangs to emerge.[105]

Lack of opportunity within a community influences the establishment and sustainment of other VNSAs. Evidence from interviews and recovered insurgent records indicates that "local, grass roots recruitment efforts centered in areas that have… limited employment opportunities."[106] In his extensive interviews with Iraqi insurgents Chehab found that higher unemployment "further inflamed" the situation.[107] In discussions with Palestinian militants in Lebanon, Cohen was continually told about the lack of opportunities present in the camps.[108] As one in particular stated:

> We can study and some of us even study outside of the camp, but for what? We can't work, we can't find jobs; we get nothing for our hard work. We feel depressed because we cannot have the opportunity for success even if we try…[109]

In the Philippines, ASG founder Abubakar Janjalani specifically targeted the vast pool of young unemployed and disaffected Muslims.[110] Regardless of location, the typical mujahid is "likely unemployed or a student (which usually amounts to the same thing)."[111]

Social Foundation

There are two ways a community's social foundation can allow and even facilitate VNSA emergence and growth: through a weak or open social foundation or through one that actually supports the VNSA. Either way, the more intertwined and accepted a VNSA becomes within a community, the stronger it is. As Epstein notes about insurgents, "the population of any given area holds the key to the success of any insurgency movement within that area."[112]

A community's social foundation is made up of the social relationships between community residents. These are formed and held together with formal and informal social ties and through social institutions like religious centers, community groups, and political agencies.[113] Bursik and Grasmick categorized these relationships as private (as in relationships among friends), parochial (as in casual relationships among neighbors that link to local groups), and public (those that link to agencies outside the community).[114] It is through these ties that a community exerts its influence over its members and what occurs within it.

A solid social foundation enables durable resistance to VNSAs. If a community has established accepted norms of behavior and community members feel free to act when these norms are violated, then VNSA development is difficult. As Sampson discovered in his research of gangs in the Chicago area, there were lower levels of crime and violence in communities that possessed greater collective efficacy.[115] Further, this collective efficacy often withstood competing influence of other structural variables. This factor was also seen operating in Iraq within what became commonly known as the "Awakening" movement. It was during this time that local Iraqi communities solidified their social foundations to actively reject unwanted insurgent elements within their communities.

The erosion of this type of solid social foundation has been found to correlate to increased VNSA activity. Gang research continually notes social instability in areas where gangs are active.[116] Fagan, for example, found that loss of intergenerational job networks was a catalyst for the disruption of the social foundations at the private and parochial levels.[117] Additionally, Vigil revealed that gang persistence was directly connected to the erosion of a "community's mechanisms for informal social control."[118] He found that economic and social marginalization of his target communities was at the heart of the degradation. A further note here: both

[102] Lafontaine, 30
[103] Klein, 214
[104] Ibid., 216
[105] Maggio, 190
[106] Watts, 7
[107] Chehab, 19
[108] Cohen, 166
[109] Ibid, 172
[110] Frake, 48
[111] Watts, 2
[112] Epstein, David G. "The Police Role in Counterinsurgency Efforts." The Journal of Criminal Law, Criminology, and Police Science 59.1 (1968): 148-151.
[113] Klein, 218
[114] Ibid.
[115] Ibid.
[116] Ibid., 216
[117] Ibid., 218
[118] Ibid.

Fagan and Vigil identified diminished economic opportunities as being related to this variable, which links it to the lack of opportunities factor discussed above.

VNSAs across the spectrum often utilize similar methods to subvert resistance by existing social foundations or to exploit those that are already weak or open. In discussing insurgents, Epstein describes these as "persuasion," "favors," and "force."[119] He further notes that, "the first steps then for any insurgent to take are those that will insure him a welcome within the mass of the people."[120] Through these methods VNSAs have quickly degraded or, in some cases, even replaced the existing dominant social forces. In researching the Saints street gang, Venkatesh discovered that:

> In effect, the Saints consciously tried to "integrate" themselves into the social fabric, using economic power as their foundation to build relations with residents and local organizations... due to this comprehensive presence – spatial, material, ideological – I argue that the early 1990's signaled the arrival of the street gang as an important element in the social organization of the… community.[121]

This is mirrored by the activity of insurgent groups like the Taliban who have replaced, overlaid or integrated into tribal social foundations in Pakistan and Afghanistan, as well as Al Qaeda related elements in Iraq who direct their members to inter-marry into host communities in order to integrate into a community's social fabric.

Weak Institutions

Communities with a rampant VNSA presence often possess weak or non-existent official institutions. Places where states or local governments refuse to or cannot effectively provide basic services leave a void that many VNSAs are eager to fill and capitalize on, further integrating themselves within the community. As such, this variable is closely tied to the social foundations variable. Examples of this are found across the spectrum of armed groups.

Gang research has identified many very clear situations where this variable is found active. Venkatesh noted a particularly stark example:

> In the void created by both Council and housing authority inaction, the Saints… channeled illicitly obtained revenues from drug economies to the general residential population. This process … had several effects on … the community: (1) it enables the Saints gang to vie for the sponsorship of resident constituencies that had previously granted their allegiance to the Council; (2) as such, the base of tenant allegiance the Councils had previously relied on was no longer self-evident, and their influence with government agencies that administered Blackstone slowly eroded because they could not unproblematically claim to be spokespersons.[122]

Positive gang contributions could be as simple and inexpensive as periodic disbursements of groceries and clothing.[123] Residents saw that the group provided a measure of public order such as enforcement, policing, escort, protection and punishment.[124] In essence, because of the official authorities' inactivity within the community, the street gang came to rival them as provider of public goods and services.[125] What resulted was the increasing and open acceptance of the gang and its illicit resources.[126]

The rise of other armed groups that reside further down the spectrum also often takes place in communities with weak official institutions and underserved populations. The groups fill the vacuums left by the incapacity of poor governments to serve and control its communities. These areas serve as the "safe havens and sanctuaries armed groups exploit to evade detection, plan operations, train forces, and stockpile supplies."[127] The discrediting and usurping of official government control is a priority of insurgencies in particular.[128] Hammes recognized that:

> In essence, these armed groups represent a return to earlier security arrangements, because a state has failed in its basic social contract of providing security for its population. These are the ethnic-sectarian militias we have seen develop around the world in response to insecurity. Groups like the Tamil Tigers and the Supreme Council for the Islamic Revolution in Iraq's (SCIRI's) Badr Militia are typical of reactionary groups.[129]

The power and service vacuums left by weak institutions promotes VNSAs across the spectrum into ever-more powerful paramilitary organizations.[130] Relatively small investments by official governments in basic services could be the easiest tools in thwarting VNSAs at their earliest stages.

Schools and Education

One of the most prevalent community services among various VNSAs is the establishment of schools and educational facilities. Parents in underserved regions are eager to give their children free educational opportunities. Not only do schools engender goodwill amongst the host community, it also provides the perfect recruiting ground for future members or supporters of VNSAs.

It is the prevalence of impressionable youth that makes schools such an attractive recruiting ground. One of the London suicide bombers, Sadiq Khan, was a mentor and assistant teacher at a school in Yorkshire

[119] Epstien, 148
[120] Ibid.
[121] Venkatesh, 92
[122] Venkatesh, 91
[123] Ibid., 96
[124] Ibid., 98
[125] Ibid., 102
[126] Ibid., 93
[127] Hanlon, 123
[128] Epstein, 151
[129] Hammes, 451
[130] Underwood, 10

and worked at a local youth center.[131] In Pakistan, some Madrassas have come under heavy criticism for "for their enrolling foreign Muslim students and for their training of a new breed of Taliban that is destabilizing the democratic government in Afghanistan and providing safe havens to Islamist militants."[132] In one case, students of the Jamia Hafsa and Jamia Faridia madrassas occupied a government building, directly challenging the Pakistani government. The stand-off resulted in a military operation and the deaths of dozens of students.

Lack of education is a prevalent, but not universal, characteristic of VNSA membership. It is also important to note here the interplay between lack of education and lack of opportunities. Economic opportunities become even more limited for those with little education. Maggio notes that regardless of race or other factors, lower education rates within a community can significantly raise the potential for street gangs to emerge.[133] Humphreys' study of VNSA activity in Sierra Leone found that education was a good predictor of membership.[134] Cohen, in talks with Palestinian militants within the Mia Mia camp, discovered that there were not enough books to go around in classrooms and teachers sometimes didn't even show up.[135] In Iraq, the insurgent Adnan Elias exhibits a typical profile. In his post-detention interview by Iraqi security forces, Elias admits to being illiterate with a 4th-grade general education before going on to describe his role in kidnapping and beheading policemen.[136]

Isolation and Marginalization

A community's actual or perceived isolation, marginalization or injustice within the larger society is commonly found in areas with a VNSA presence. This element can feed into and amplify a group's oppositional culture. In Sierra Leone, VNSA members were most often those that were "marginalized from political decision making… alienated from mainstream political processes."[137] Humphreys' analysis found a strong correlation between recruitment and alienation from the system. Individuals who were not connected to any political party were two to three times more likely to join VNSAs.[138]

Gang research shows similar findings. Vigil, for instance, revealed that both the "social and economic marginalization" of immigrant communities played a significant role in gang emergence.[139] In some cases the communities perceive not just marginalization but active hostility. Within the Chicago gang area Venkatesh studied, community members perceived themselves as an isolated community amidst hostile official authorities.[140] Jihadist groups looking to recruit insurgents for Afghanistan and Iraq focused on areas that exhibited some form of social isolation.[141] As Jessica Stern describes about the making of terrorists, "there's a very strong feeling of… profound injustice that the terrorist leaders are capitalizing on."[142] Paul Wilkinson describes it as "nursing grudges".[143]

Variable Interdependence

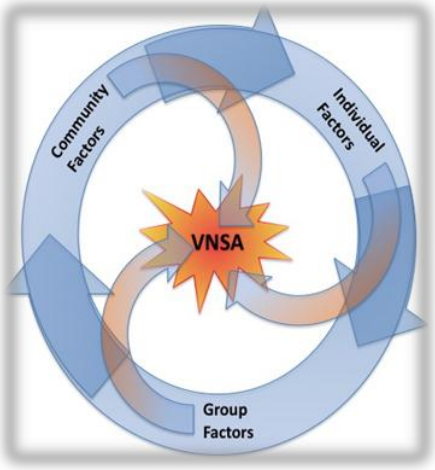
A review of common variables and characteristics indicates that many individual and group similarities are sourced in or tied to community-level issues. There is heavy interdependence between the lower levels and a community's lack of opportunities, weak social foundations, weak official institutions, and isolation or marginalization. These all clearly hold heavy influence on individual level factors such as seeking purpose, identity issues, status, respect, power and free time and boredom. It also can be easily tied to group level factors like oppositional culture.

Gang researchers and counter-gang practitioners have noticed this correlation as well. Klein and Maxson recognized that, "the main problem with street gangs in the long run is not the gangs themselves, but the societal and community processes that spawn these gangs."[144] This suggests that the community-level variables are the primary targets of counter-VNSA efforts and must be addressed first if a lasting impact is desired.

However tantalizing it is to ascribe a singular variable to VNSA membership, each aspect (individual, group and community) is interdependent and each impacts an individual's motivations to varying degrees. A recent article on street gangs recognizes this interplay:

> If a young adult is devoid of opportunities for advancement and the possibility to earn respect and develop an identity/purpose in his/her life, in addition to missing positive social influences the young adult is left vulnerable to filling these voids through socially undesirable outlets. Gang culture is one realm in which these voids may be filled in a relatively immediate manner for these young adults. It gives them a sense of belonging, identity, and a purpose.

[131] Herbert, Ian. Panel discussant. "The Making of a Terrorist." Talk of the Nation. Hosted by Neal Conan. 18 Jul 2005.
[132] Tufail, Ahmad. "Inquiry and Analysis No. 462." MEMRI. Accessed 23 Jan 2009.(http://www.memri.org/bin/articles.cgi?Page=subjects&Area=urdu&ID=IA46208)
[133] Maggio, 190
[134] Humphreys, 447
[135] Cohen, 166
[136] Elias, Adnan. Interview on Al-Iraqiya TV. 20 Apr 2005. Accessed 23 Jan 2009. (http://www.memritv.org/clip/en/0/0/0/0/0/144/650.htm)
[137] Humphreys, 440
[138] Ibid., 447
[139] Klein, 218
[140] Venkatesh, 101
[141] Watts, 7
[142] Stern
[143] Wilkinson, Paul. Panel discussant. "The Making of a Terrorist." Talk of the Nation. Hosted by Neal Conan. 18 Jul 2005.
[144] Klein, 106



The VNSA Variable Interdependence Cyclone

Conclusion

International security experts have recognized the rising similarities between different forms of non-state violent groups. This has led to a blurring of lines between what were previously considered distinct categories of groups. In turn, this blurring has suggested that there might be more fundamental likenesses between groups with potential implications for decisions on how to counter them.

Comparing the vast amount of existing gang research and counter-gang experience to current knowledge of other forms of VNSAs reveals common variables and characteristics at the individual, group and community levels of analysis. It suggests the supreme importance of community level variables in addressing VNSAs. Further, analyzing counter-gang experience and research can provide fresh insight into countering other VNSAs.

Armed non-state groups are a growing challenge to modern international and domestic security. Understanding the nature of and similarities between VNSAs at the individual, group and community levels is central to countering this increasingly dangerous security challenge.

An Assessment of UK Anti-Terrorism Strategy and the Human Rights Implications Associated with its Implementation

Emmanouela Mylonaki and Tim Burton, CPS

Introduction

Following 9/11, anti-terrorism legislation in the United Kingdom became more stringent, thus widening the scope of offences that qualify as terrorist acts and encroaching on the human rights and fundamental freedoms of the accused. Despite the distinction between the terms 'anti-terrorism' and 'counter-terrorism' they are often used interchangeably. Whereas counter-terrorism broadly refers to offensive measures of a preventive, deterrent and pre-emptive nature, anti-terrorism refers to the construction and use of defensive measures to reduce a terrorist threat.[1] Anti-terrorism, by definition, is therefore narrower in scope.

The varied nature of terrorist offences necessitates a range of governmental responses, which poses difficulties in evaluating the effectiveness of the UK anti-terrorism strategy by using a universal methodology.[2] Instead a comparative approach is used to identify similarities between the anti-terrorism strategy in the United Kingdom and the United States. Besides the effectiveness of a strategy in achieving its political aims, legitimacy and public confidence are equally important factors, and thus emphasis is places on such factors.[3]

Evolution of the United Kingdom Anti-terrorism Strategy

The complex nature of terrorism indicates that there is a need for a multifaceted strategy which, ideally, upholds the rule of law and liberty.[4] Since 2001, the UK anti-terrorism strategy has substantially changed as highlighted in Tony Blair's pronouncement that the 'rules of the game' were changing with his 12-point plan addressing extremism and its causes.[5] Lately Gordon Brown's statement to the House of Commons outlined the government's response to 'global international terrorism' by the introduction of new powers and terrorism-related offences.[6]

Post-2001 there has been an increased use of executive powers as an alternative strategy to prosecution. The House of Lords declared section 23 of the Anti-terrorism, Crime and Security Act 2001 (ACTSA 2001)[7] as incompatible with the European Convention on Human Rights (ECHR). Such incompatibility was based on the grounds that part 4 of the ACTSA powers were discriminating against foreign nationals. The UK governmental response was to replace part 4 of the UK act with a new system of control orders.[8]

From 2003 onwards, the UK government has been particularly active in the fight against terrorism as evident by the adoption of the two versions of the UK counter-terrorism strategy known as 'CONTEST' strategy. 'CONTEST' 1 comprises four elements: Prevention, Pursuit, Protection, and Preparedness.[9] When the strategy was announced the role of anti-terrorism legislation was described as the framework within which to 'dismantle the machinery of terrorism'.[10] The present article focuses on the 'prevent' and 'pursuit' strands of this strategy.

The 'prevent' strand includes deterrence measures to prevent those who 'facilitate terrorism' and 'encourage others'[11], with the purpose of making it more difficult for terrorists to operate.[12] The Terrorism Act 2000 (TA 2000) with its proscription provisions and the Terrorism Act 2006 (TA 2006) with offences of encouragement and glorification of terrorism and dissemination of terrorist publications fall within these deterrence measures under the 'prevent' strand.[13] As will be seen, the broad reach of the legislation is able to target individuals who are not terrorists. This carries the danger of radicalising innocent victims into becoming terrorists.

Prosecution is aimed at disrupting terrorist activity and falls within the 'pursuit' strand.[14] Since the aim of 'pursuit' is to reduce the terrorist threat both to the UK and overseas [15] this extends to include alternative measures of control such as prosecution and

[1] US Department of Defence Dictionary of Military and Associated Terms (as amended 31 October 2009) http://www.dtic.mil/doctrine/dod_dictionary/ accessed 07 March 2010.

[2] B Hoffman and J Morrison-Taw, A Strategic Framework for Countering Terrorism in F Reinares (ed), European Democracies Against Terrorism: Governmental Policies and Intergovernmental Cooperation (Aldershot Ashgate 2000), p.p. 3-7.

[3] Ibid, p.p. 8 – 19.

[4] P Heymann, Terrorism and America A Commonsense Strategy For A Democratic Society (The MIT Press, Cambridge Massachusetts 1998), p. p. 153 – 154.

[5] PM's Press Conference 5 August 2005 www.number10.gov.uk/output/Page8041.asp accessed 28 February 2010.

[6] Statement on security and counter-terrorism 20 January 2010 , www.number10.gov.uk/output/Page22206.asp accessed 28 February 2010.

[7] A v Secretary of State for the Home Department [2004] UKHL 56; [2005] 2 AC 68.

[8] 'Measures to Combat Terrorism – powers in Part 4 of the Anti-terrorism, Crime and Security Act 2001' Oral Statement by Charles Clarke, the Home Secretary, in January 2005 , http://press.homeoffice.gov.uk/Speeches/speeches-archive/st-combat-terrorism-0105 accessed 03 May 2010.

[9] HM Government, 'Countering International Terrorism: the United Kingdom's Strategy' (Cm 6888 London TSO 2006) p. 1 para. 5 and p. 5 para. 22.

[10] *H Blears, The Tools to Combat Terrorism, Speech to the Royal United Services Institute in February 2005, http://press.homeoffice.gov.uk/Speeches/speeches-archive/sp-tools-combat-terrorism-0205 accessed 01 May 2010.*

[11] Supra note 9, p. 1, para. 6.

[12] Ibid, p. 12 para. 50.

[13] Ibid, p.11, para.50.

[14] Ibid, p. 2, para. 7.

[15] Ibid, p. 16 para. 64.

deportation.[16] Prosecution in itself is recognised to have indirect effect. For example, prosecuting non-terrorist offences such as fraud can further disrupt terrorist networks.[17] Whilst the reduction of the terrorist risk is the main aim of the strategy, there is a willingness to extend the ambit of prosecution and also use executive measures as alternatives to prosecution. This raises important issues about the net-widening effect of the strategy, its legitimacy, and its adherence to human rights standards. It is clear that the strategy is not limited to prosecution since 'security measures' are to be taken where the prosecution of offences is not possible.[18] This aspect of the strategy demonstrates its flexible and invasive nature. For example, deportation is a measure under both the pursuit [19] and prevent[20] strand.

The strategy points out the results that prosecution has delivered in 'disrupting terrorist activity', as was evident in the cases of Mohammed Khan, Abu Hamza, Andrew Rowe, Saajid Badat, and Kamel Bourgass.[21] The Home Office (lead government department for counter-terrorism) data on prosecution is revealing. There have been 310 prosecutions from 2001-2008 with a 74% conviction rate[22] raising to 86% for the 29 terrorism trials in 2009.[23] However, this 'success' rate masks a difference. For example, the percentage of those 1,759 terrorism arrests since 11 September 2001 resulting in charge and conviction is 13%[24] and of-201 arrests for the year ending September 30th, 2009, 66 were charged with the majority being non terrorism related offences (42) and only 17 directly charged under the terrorism legislation.[25] This suggests emphasis on prosecuting people believed to be associated with terrorism. Indeed, since 2001, 30% of the main charges under terrorism legislation have been for possession of an article for terrorist purposes (such as documents, compact discs or computer hard drives), 14% for fundraising for illicit activity and 12% for membership of a 'proscribed organisation.'[26] This shift away from prosecuting terrorism under terrorism legislation is becoming a more prevalent strategy for countering terrorism. This is demonstrated by a similar shift in the United States towards trying suspected terrorists with non-terrorism offences.[27] Only 32% of indictments in terrorism trials contained terrorism offences [28] under the US terrorism statutes.[29] Post 9/11, the US Department of Justice increased the use of terrorism related charges[30] and non-terrorist charges[31] as a means to prevent terrorist attacks by disrupting terrorist networks. This strategy in the United States has also led to increases in non-terrorist charges such as identity theft and immigration frauds as a design to emasculate those identified in a terrorism investigation.[32] Therefore, strategies for dealing with terrorism have evolved to use a greater range of legal powers to target not simply terrorists and acts of terrorism, but activities facilitating the organisation and operation of terrorists.

Likewise, the UK strategy has taken this direction. Haubrich illustrates the comparative rarity of terrorism charges. For example there was not a single charge under ACTSA 2001 between September 2001 and 2005.[33] He also argues that the TA 2000 enables prosecutors to extend the reach of terrorism prosecution.[34] As Haubrich argues, this result in more people brought into the ambit of terrorism and criminalised as terrorists.[35] This similarity of the UK strategy to the United States strategy emphasises that the 'War on Terror' has extended its reach to people who are not terrorists and extended its reach to acts which are not necessarily acts of terrorism. Extending the reach of the UK strategy to the prosecution of anyone deemed to be associated with terrorism makes the anti-terrorism measures of a counter-terrorist nature moving towards deterrence and aggressive prosecution.

National Security Strategy in the United Kingdom

Terrorism is one of a number of security challenges that can be included within an overarching strategy. There is now an identifiable change of approach where the anti-terrorism strategy, as one of a number of security challenges (also transnational crime, global instability, civil emergencies, foreign states, nuclear weapons), is brought within a composite strategy. The

[16] Ibid, p. 17 para. 69.
[17] Ibid, p. 17 para. 70.
[18] Ibid, p. 18 para. 72.
[19] Ibid, p. 18 para. 73.
[20] Ibid, p. 12.
[21] Ibid, p. 18 para. 71.
[22] Home Office, 'Operation of Police Powers under the Terrorism Act 2000 and subsequent legislation: Arrests, outcomes and stops & searches Quarterly update to September 2009 Great Britain' (Home Office Statistical Bulletin 04/10 25 February 2010) Table 1.4 p. 10 http://www.homeoffice.gov.uk/rds/pdfs10/hosb0410.pdf accessed 11 March 2010.
[23] Ibid, Table 1.5 p. 11.
[24] Ibid, Table 1.5, p.5.
[25] Ibid, Table 1.2 p. 8.
[26] Ibid.
[27] J Grossman (ed), Terrorist Trial Report Card: September 11, 2001 – September 11, 2009 (The Center on Law and Security, New York University School of Law 2010) executive summary (ii) 'the evolving record' http://www.lawandsecurity.org/publications/TTRCFinalJan14.pdf accessed 03 May 2010.
[28] Ibid, p. 4.
[29] Ibid, p. 5. The primary terrorism statutes are listed as: 18 U.S.C. 2332 (Terrorism); 18 U.S.C. 2339A (Material Support to Terrorists); 18 U.S.C. 2339B (Material Support to a Foreign Terrorist Organization); 50 U.S.C. 1705 (Financial Support to a Foreign Terrorist Organization) http://www.lawandsecurity.org/publications/TTRCComplete.pdf accessed 11 March 2010.
[30] K Wainstein, Terrorism Prosecution and the Primacy of Prevention Since 9/11 in J Grossman (ed) Terrorist Trial Report Card: September 11, 2001 – September 11, 2009 (The Center on Law and Security, New York University School of Law 2010) page 21 http://www.lawandsecurity.org/publications/TTRCFinalJan14.pdf accessed 03 May 2010.
[31] Ibid.
[32] Supra note 27, p. 22.
[33] D Haubrich, Anti-Terrorism Laws And Slippery Slopes: A Reply To Waddington (2006) Policing and Society 16 (4) 405, p. 408.
[34] Ibid, p. 409.
[35] Ibid, p. 411.

2008 National Security Strategy[36], which conceptualises national security in the UK, has elevated terrorism from a threat to state security to a concept encompassing threats to the population[37] and an attack on values.[38] The shift is from legislative response to public engagement[39] whilst the government targets international extremism.[40] A new concept is 'interdependence' whereby the transnational and international aspects of terrorism intersect [41] so there is a universal response addressing all threats to security. [42] For example, the strengthening of borders and the National Identity Scheme tackles both terrorism and transnational crime.[43] The new face of terrorism as embodied by Al Qaeda is the diffusion of a common ideology resulting in a loose 'network of affiliated groups'[44] and includes autonomous groups.[45] Making such terrorism threats part of a national security strategy shows that a separate anti-terrorism strategy is no longer tenable. However, the problem with this national security approach is finding a right balance between security and liberty.[46]

The United States has a centralised Department of Homeland Security, whereas the UK relies on the 'lead government department' model for domestic security issues.[47] In other words the department with expertise responds to the current crisis.[48] Some argue that the UK strategy can work without a 'homeland security' department;[49] however, the absence of such a department makes it difficult to react to domestic security issues.[50]

Whatever the merits of either model, it is recognised that the terrorist threat no longer neatly divides into national and international problems.[51] However, the difficulty is combining the two particularly in the case of a 'homeland security' model.[52] A generic problem is the role of the public in domestic security. [53] It is this generic problem combined with the issue of moral legitimacy which raises questions about the efficacy of the UK strategy. The UK NSS has been criticised as not describing a meaningful strategy in terms of how its aims and values[54] will be delivered.[55] Although the UK is considered to have acknowledged the challenges brought about by the increase in transnational and international terrorism, the National Security Strategy does not set out a strategy to deal with these challenges.[56] Although recognised that the terrorist threat no longer divides into national and international and requires a national security approach,[57] the NSS has been criticised as being unclear as to how its aims will be delivered.[58] That the terrorist threat is considered by the UK government to not amount to a strategic threat to the UK[59] is at odds with the 'War on Terror'[60] doctrine according to which terrorism threat should be perceived as a strategic threat to the UK. This reflects the difficulty with attempting to combine national and international strategy.[61] Reducing the terrorist threat to one which does not affect the UK strategically, raises questions as to whether it is legitimate for the UK to apply the 'War on Terror' approach to the national prosecution of international terrorism.

Changes to the National Security in the United Kingdom Post 9/11

The revised CONTEST strategy echoes the NSS with the emphasis now on public participation. Thus, the anti-terrorism strategy can be seen to be no longer purely a legislative response. Public participation is now emphasised as central to successful delivery of the strategy, with responsibility for rejecting extremism being made the responsibility of everyone.[62] Also the 'prevent' strand has expanded[63] to prevent terrorism at an earlier stage with the aim to stop people from joining the terrorist cause.[64] The concept of a working partnership has been developed in which communities are empowered to assist in the fight against terrorism.[65] The key difference is the wholesale revision of the 'prevent' strand[66] to prevent individuals becoming terrorists and stop people from supporting violent extremism.[67] Despite commitments made by the UK

[36] Cabinet Office, 'The National Security Strategy of the United Kingdom – Security in an interdependent world' (Cm 7291 London TSO 2008).
[37] Ibid, p. 3 para.1.5.
[38] Ibid, p. 28 para.4.14.
[39] Ibid, p. 26 para. 4.8 – 4.9.
[40] Ibid, p. 27 para. 4.10.
[41] Ibid, p. p 23 -24 para. 3.53 and para. 3.54.
[42] Ibid, p. 24 paragraph 3.57.
[43] ibid p.p. 56 – 57 para. 4.109 and para. 4.110.
[44] A Zelinsky and M Shubik, Research Note: Terrorist Groups as Business Firms: A New Typological Framework, (2009) 21 Terrorism and Political Violence, p. 327 .
[45] A Kirby, The London Bombers as "Self-Starters: A Case Study in Indigenous Radicalization and the Emergence of Autonomous Cliques, (2007) 30 Studies in Conflict and Terrorism 415, p. 426.
[46] J Baker, In The Common Defense National Security Law For Perilous Times (Cambridge University Press 2007), p. 11.
[47] F Gregory, National governance structures to manage the response to terrorist threats and attacks in P Wilkinson (ed), Homeland Security in the UK (Routledge 2007), p.p. 117 – 119.
[48] Ibid, p. 119.
[49] Ibid, p. 135.
[50] Ibid, p.p.132 – 133 and p. 136.
[51] Supra note 46, p. 251.
[52] Ibid, p.p.. 252 – 253.
[53] Supra note 47, p. 123.
[54] J Gow, The United Kingdom National Security Strategy: the Need for New Bearings in Security Policy, (2009) 80 (1) The Political Quarterly 126, p. 131.
[55] Ibid, p.p. 127 – 128.
[56] Ibid, p.129.
[57] Supra note 46, p. 251.
[58] Supra note 54, p.p. 127 – 128.
[59] Cabinet Office, 'The National Security Strategy of the United Kingdom – Security in an interdependent world' (Cm 7291 London TSO 2008), p. 11 para. 3.9.
[60] Supra note 54, p. 129.
[61] Supra note 46, p.p. 252 – 253.
[62] HM Government, 'The United Kingdom's Strategy for Countering International Terrorism' (Cm 7547 London TSO 2009) p. 57 and p. 87.
[63] Ibid, p. 58 para.7.11.
[64] Ibid, p. 87.
[65] Ibid, p. 84 para. 9.12 and para. 9.13.
[66] Ibid, p. 58 para. 7.11.
[67] Ibid, p. 87.

government to the protection of human rights, its anti-terrorism strategy fails to 'preserve and protect' the freedom of assembly and association, and freedom of thought, conscience and religion as provided for within Articles 10, 11 and 9 (respectively) in the ECHR. The UK Government does, however, acknowledge that the right to 'thought and speech' will not be criminalised.[68]

The anti-terrorism strategy has moved beyond confronting cause and effect to altering the conditions in which terrorism is thought to flourish.[69] Although CONTEST's approach is a robust approach aimed at removing the threat of terrorism, it is also capable of being used against all political beliefs. This is evidenced, for example, by reference to a 2008 Police Strategy where staff will work with neighbourhood policing teams to 'identify and take action against individuals' deemed to be exploiting vulnerable people.[70] If this fails then the UK Border Agency will use powers of exclusion and deportation including UK residents.[71] Moreover, the Home Secretary will invoke the power to either revoke British citizenship or exclude foreign nationals from entering the UK.[72] This illustrates that maintenance of national security comes at a price to the preservation of values of freedom of expression and freedom of movement. However, it should be noted that such preventive approach is unprecedented and due to its novelty it is too soon to evaluate it in terms of success/failure.[73] But at this stage, one can argue that the wide ranging nature of the strategy creates the real danger of seen terrorism activity wherever the authorities turn their attention to. Despite the UK government's intention to use only proportionate measures, there is a risk that the expansion of the strategy will target any ideologically motivated activity (for example riots) as well as terrorism.[74] Thus, the measures adopted may no longer be proportionate. In addition, CONTEST does not consider the negative impact the measures may have in radicalising people.[75] However, the UK strategy is not dissimilar to the European Union (EU) Counter-Terrorism Strategy based on similar four strands with an objective to stop recruitment and radicalisation.[76]

Under the 'pursue' strand executive measures are still perceived as a necessary alternative to prosecution.[77] In particular control orders continue in spite of judicial challenge[78] with an increase of 15 orders as of December 10th, 2008 to 40 as at March 10th, 2009.[79] Proscription and asset freezing remain in place and[80] and the Counter-Terrorism Act 2008 is seen to enhance asset-freezing powers in addition to increasing police investigative powers.[81] The strategy, therefore, continues the existing framework of combining legislative and executive measures. The continuous use of executive measures raises concerns as the measures may become a permanent feature of anti-terrorism strategy, even when the justification for their use has passed.

Official assessment of the system ignores the human rights implications. The UK Parliament Home Affairs Committee in reviewing the dual structure of strategic delivery by the Office for Security and Counter-Terrorism[82] and police responsibility for anti-terrorist operations[83], reported confidence in this system.[84] Reporting on CONTEST in 2010 the government, unsurprisingly, suggested that the strategy achieved its aims.[85] However, there is no mechanism to make independent evaluation of CONTEST because the Public Service Agreement assessments are classified information.[86] Moreover, the UK Parliament Home Affairs Committee did not provide any coherent evidence that it was successful in stopping extremism.[87] The strategy however, has run into problems as evidenced by negative court rulings such as the January 2010 ECHR ruling against section 44 of the Terrorism Act 2010[88] and the Supreme Court ruling against asset freezing using secondary legislation.[89] The UK government responded by saying that the ECHR ruling would be appealed and emergency legislation has restored asset freezing with further legislation to follow, in order to combat terrorism financing.[90] This further demonstrates that the strategy is unyielding.

Some argue that CONTEST has upheld liberty.[91] For example Kostakopoulou argues that the UK's post 9/11 response has been narrowly proscribed in its 'security narrative' approach and its construction displays 'a siege mode of democracy'.[92] She further argues that this replaces a rights-based model where human rights are

[68] Ibid, p. 87.
[69] Ibid, p. 56 para. 7.03.
[70] Ibid, p. 85 para. 9.16.
[71] Ibid, p. 89.
[72] Ibid, p. 66, para. 8.19 -8.22.
[73] Ibid, p. 99.
[74] Ibid, p. 56 para. 7.03.
[75] C Pantazis and S Pemberton, Policy Transfer and the UK's 'War on Terror': A Political Economy Approach, (2009) 37(3) Policy and Politics 363, p.368.
[76] The EU Counter Terrorism Strategy 14469/4/05 REV 4 Brussels 30 November 2005 paragraph 6 http://register.consilium.eu.int/pdf/en/05/st14/st14469-re04.en05.pdf accessed 21 April 2010.
[77] Supra note 75, p. 66 para.8.18
[78] Supra note 62, p. 68 para.8.33 – 8.34.
[79] Ibid, p. 68, para. 8.35.
[80] Ibid, p.68 para 8.36-8.37
[81] Ibid, p. 69 para. 8.41.
[82] http://www.security.homeoffice.gov.uk/about-us/ accessed 03 May 2010.
[83] Home Affairs Committee, 'Project CONTEST: The Government's Counter-Terrorism Strategy' Ninth Report [Session 2008-09] HC (2008-09) 212 Ev 22 Charles Farr OBE Q132 http://www.publications.parliament.uk/pa/cm200809/cmselect/cmhaff/212/212.pdf accessed 03 April 2010.
[84] Ibid, para. 15 - 16.
[85] HM Government, 'The United Kingdom's Strategy for Countering International Terrorism Annual Report March 2010' (Cm 7833 Norwich The Stationery Office 2010) p. 27.
[86] Ibid, p.26 para. 7.02 and 7.04.
[87] Ibid, p. 12 para. 3.02.
[88] Gillan and Quinton v The United Kingdom [2009] ECHR 28 12 January 2010 Application no 4158/05.
[89] A v HM Treasury and Others [2010] UKSC 2.
[90] Supra note 86, p. 9 para. 2.05 and p. 10 para. 2.12.
[91] Ibid, p. 157.
[92] D Kostakopoulou, How To Do Things With Security Post 9/11, (2008) Oxford Journal of Legal Studies 28(2) 317, p. 319.

observed and respected.[93] Further, she advocates the need to move away from the 'War on Terror' approach.[94] Perhaps the UK strategy has moved away from the 'War on Terror' approach by advocating risk management[95] and encouraging the public to become more involved. However, its basis is the anti-terrorism legislative framework, itself the legacy of threat and response. As Kostakopoulou argues, this legacy means greater potential interference to liberty because the enabling effect is to spread the strategic response to the threat outwards to all aspects of society beyond terrorism.[96]

Executive Measures of the UK's National Security Strategy Post 9/11

Perhaps the conflict between the rights of the individual and the government's duty to protect to protect the public right to life under Article 2 ECHR [97] becomes clear by reference to the imposition of 'control orders' by the UK Home Secretary. Such orders may be imposed against an individual and contain obligations on him restricting his liberty, freedom of association and use of services.[98] In *AF & Others* Lord Hoffmann commented that upholding the rule of law and safeguarding against wrong decisions may not provide adequate public protection.[99] Although public protection is the purpose of control orders, as Lord Scott points out, the duty of the courts is not to protect the public but to apply the law.[100] These contrasting duties emphasise the difficulty with reconciling Human Rights and security.

British courts have openly ruled against the imposition of control orders. In AF v Others where it was decided that the controlee has to know the substance of the allegation against him[101] two orders were revoked and then replaced with new orders containing fewer conditions.[102] The judicial decisions against control orders challenge the validity of them and trigger questions as to the continuation of the application of control orders. The opinion of Lord Carlile (independent reviewer of control orders) in reviewing such orders is that orders should be the exception[103] and only apply to substantial risk cases.[104] He is critical of the 'light touch' practice, interpreting this as being used to avoid disclosure of the evidence upon which the orders were issued.[105] Proportionality is also an issue because Lord Carlile suggested only the minimum number of obligations necessary to meet public safety is imposed.[106] His idea of limiting the categories of cases in which control orders apply was rejected in the government's reply to Lord Carlile's report.[107] The consequence of the 'light touch' orders is the control order system now contains different criteria for making orders. The government is reluctant to abandon this system, despite acknowledging that the practice of 'light touch' orders is difficult to justify.[108]

Control orders can be "non-derogating" made by the Secretary of State under section 2 of the Prevention of Terrorism Act 2005 (PTA 2005), which means that the restrictions they contain do not involve derogating from the ECHR. Or they can be "derogating" under section 4 of the PTA 2005 where the proposed restrictions involve derogating from the ECHR and are made by the court on application from the Secretary of State. Non-derogating orders should last for 12-months with renewal only if necessary for public protection.[109] Lord Carlile has questioned the UK practice of repeated renewal of non-derogating control orders.[110] The government previously rejected his proposal of a presumption against extension beyond 2 years.[111] This illustrates the difficulty with executive measures embedded in a permanent strategy and those measures taking on a permanent quality. Once a control order has been made, the police are under a duty to keep criminal prosecution as a possibility.[112] However, it follows that a control order which is effective should prevent criminal offences occurring and therefore there will be no need to prosecute the person subject to the control order. Therefore, the continuation of the order becomes justified because of its effectiveness in preventing criminal offences. Indeed, Walker has stated that 'no one subject to an order has subsequently been prosecuted as an alternative to the order'.[113]

Whilst the emphasis has been on the procedural fairness in imposing control orders, it is questionable whether the control order regime is fully compliant with ECHR rights. On the fifth renewal of the regime[114] the UK Parliament Joint Committee on Human Rights view was that the system is no longer sustainable. This is due to the fact that the system could not guarantee procedural fairness and is interfering with ECHR Article 5 right to liberty.[115] Case law raises this question of interference

[93] ibid, p. 322.
[94] Ibid, p. 341.
[95] Ibid, p. 322.
[96] Ibid, p. 334.
[97] AF & Others [2009] UKHL 28 per Lord Hope paragraph 76, Osman v UK Application No 23452/94 28 October 1998 (2000) 29 EHRR 245.
[98] Section 1(1) and 1 (4) Prevention of Terrorism Act 2005.
[99] AF & Others [2009] UKHL 28 per Lord Hoffman paragraph 70 – 74.
[100] AF & Others [2009] UKHL 28 per Lord Scott paragraph 91.
[101] AF & Others [2009] UKHL 28 per Lord Philips paragraph 57 – 69.
[102] Home Office, 'The Government Reply To The Report By Lord Carlile' (Cm 7855 London The Stationery Office 2010) p. 8.
[103] Lord Carlile, 'Fifth Report Of The Independent Reviewer Pursuant To Section 14 (3) Of The Prevention Of Terrorism Act 2005' (London The Stationery Office 2010) p. 1 and p. 34 para. 96.
[104] Ibid, p. 31 para. 85.
[105] Ibid, p. 30 paragraph 84.
[106] Ibid, p. 12 para. 21, p. 30 para. 84, p. p. 41 – 42 para. 118.
[107] Home Office, 'The Government Reply To The Report By Lord Carlile' (Cm 7855 London The Stationery Office 2010), p. 1.
[108] Ibid, p. 8.
[109] Section 2 (6) Prevention of Terrorism Act 2005.
[110] Supra note 104, p.p. 43 – 44, para. 121.
[111] Ibid, p. 45 para. 124.
[112] Section 8 (4) Prevention of Terrorism Act 2005.
[113] C Walker, The Threat of Terrorism and the Fate of Control Orders, (2010) Public Law Jan 4, p. 6.
[114] Prevention of Terrorism Act 2005 (Continuance in force of sections 1 to 9) Order 2010.
[115] Joint Committee on Human Rights, 'Counter-Terrorism Policy and Human Rights (Sixteenth Report): Annual Renewal of Control Orders Legislation 2010 [9th Report Session 2009-10] HL

and proportionality. With restrictions of curfew on the time a controlled person can be out of his house, the point at which this becomes a deprivation of liberty is arbitrary when *Secretary of State for the Home Department v JJ & Others* [116] is considered. Whilst reaching the conclusion that 18- hour curfews breached Article 5, Lord Brown was of the view that 12-14 hours did not constitute a breach of Article 5 and regarded 16 hours as the acceptable limit.[117] It is difficult to see what makes 16 hours the acceptable limit where 18 hours is regarded as a loss of liberty.[118] On the other hand Lord Bingham took the view there was no dividing line[119] in deciding that curfew conditions amounted to solitary confinement.[120] The Joint Committee voiced concerns about this impact of control orders on lives.[121] Thus, the ECHR Article 8 right of respect for private and family life is also engaged.[122] In giving evidence before the Committee, human rights lawyer Gareth Peirce pointed out that although the orders may only affect a small number of individuals, the wider impact was a sense of injustice.[123] This argument is based on the fact that control orders operate outside the criminal justice system and challenge principles such as the presumption of innocence and the right of a fair trial. Therefore, legitimacy is in question. Indeed the Joint Committee was critical of the increased practice of relocating individuals to other areas of the country as part of 'light touch' orders.[124]

There is now a serious issue about the compatibility of control orders with ECHR rights. This follows the recent ruling of the UK Supreme Court recently in *R (on the application of AP) v Secretary of State for the Home* Department.[125] The relocation of *AP* from London to the Midlands with the purpose of removing him from associating with Islamist extremists in London meant that those restrictions to his ECHR Article 8 right was a factor relevant to the issue of whether the control order breached ECHR Article 5 right to liberty. Therefore, ECHR Article 8 rights could be a decisive factor in tipping the balance in respect of ECHR Article 5.[126] Judge Lord Brown also found that in considering whether a control order amounts to the deprivation of liberty subjective factors and person specific factors – such as the difficulty of family visits – could be taken into account.[127] In spite of this, Lord Brown continues to hold the view that other conditions 'would have to be unusually destructive of the life' of the controlee for a control order to amount to a deprivation of liberty as opposed to merely a restriction on liberty.[128] Yet in acknowledging the interaction of ECHR rights and acknowledging that factors specific to the individual could be taken into account, the argument about the proportionality of control orders becomes difficult to sustain. If the balance can be tipped by the restriction to the ECHR Article 8 right to family life, then to hold this as only a deprivation of liberty if 'unusually destructive' of the life of the controlee is to fail to acknowledge the terms of ECHR Article 5.

Where control orders are concerned, the deprivation of liberty under ECHR Article 5(1) (c) is permitted where the measure 'is reasonably considered necessary to prevent his committing an offence'. In the European Court of Human Rights case of *Guzzardi v Italy*[129] this phrase was considered to be limited to giving States a means to prevent 'a concrete and specified offence'.[130] Neither does the ECHR Article 5 (1) (b) exception of detention 'to secure the fulfilment of any obligation prescribed by law' apply where general obligations are imposed by the legislative measures.[131]

The debate on the use of executive measures highlights that-there is no middle ground between security and liberty. The anti-terrorism strategy is skewed towards executive control founded on intelligence.[132] The one-sided choice between prosecution and executive control is a consequence of managing the terrorist threat.[133] The limitation is that this reduces the protection of individual liberties. Having considered the question of alternatives to control orders, many academics such as Walker suggested the use of surveillance.[134]

The use of banning named terrorist organisations ('proscription') is another executive measure which raises Human Rights issues. The 2010 CONTEST Report states that such measures help to make the UK 'a more hostile environment for terrorism'.[135] However, when proscription was part of the former Prevention of Terrorism (Temporary Provisions) Act 1989 the efficacy of such measures was doubted. Walker described proscription as a measure which was purely symbolic intended to put terrorist organisations out of public sight.[136] The difference now is that by Section 1 (4) of the TA 2000, proscription is extended to international

64 HC 395, p. 34 para. 111 – 112. http://www.publications.parliament.uk/pa/jt200910/jtselect/jtrights/64/64.pdf accessed 11 April 2010.

[116] [2007] UKHL 45.

[117] [2007] UKHL 45 at para. 105.

[118] [2007] UKHL 45 per Lord Brown at para. 108.

[119] [2007] UKHL 45 at para. 17.

[120] [2007] UKHL 45 at para. 24.

[121] Supra note 116, p. 16 para. 44.

[122] [2007] UKHL 45 per Lord Hoffmann at paragraph 34.

[123] Supra note 122.

[124] Ibid, p. 5 para. 41.

[125] [2010] UKSC 24; [\2010] 3 WLR 51.

[126] R (on the application of AP) v Secretary of State for the Home Department [2010] UKSC 24; [2010] 3 WLR 51 per Lord Brown at para 12.

[127] Ibid, para 15 and para. 19.

[128] R (on the application of AP) v Secretary of State for the Home Department [2010] UKSC 24; [2010] 3 WLR 51 per Lord Brown at para 4.

[129] (1981) 3 EHRR 333.

[130] Guzzardi v Italy (1981) 3 EHRR 333 at para 102.

[131] Ibid, para 101.

[132] C Walker, Intelligence and Anti-terrorism legislation in the United Kingdom, (2005) 44 Crime Law and Social Change 387, p.p. 387 – 390 and p. 413.

[133] D Bonner, Executive Measures, Terrorism and National Security (Ashgate 2007) p.p. 214 – 216.

134 Supra note 132

[135] HM Government, 'The United Kingdom's Strategy for Countering International Terrorism Annual Report March 2010' (Cm 7833 Norwich The Stationery Office 2010) p. 10 para. 2.10.

[136] C Walker, The Prevention of Terrorism in British Law (2nd edn Manchester University Press 1992) p. 64.

organisations.[137] Walker considers that proscription had limited value on the grounds this can drive an organisation underground.[138] In his latest report on the operation of the TA 2000, Lord Carlile echoes the doubt about the value of proscription, reporting that proscription does little to protect the public other than to label dangerous organisations and provide grounds to prosecute 'lower level activity'.[139] Similar doubts have been raised by various scholars.[140] Proscription is considered by the government to be essential to addressing militant radicalisation, as evidenced by the recent proscription of Al Muhajiroun.[141] It remains to be seen what effect this will have on preventing radicalisation. Out of 80 convictions under the TA 2000 since September 11th, 2001, 15 were for sections 11 to 13 offences of membership and support of proscribed organisations and the wearing of uniform in public. There were no convictions in 2003 to 2005 or in 2008 to 2009.[142] Yet the list of proscribed international organisations grew to 45 at the end of 2008.[143] This growth in the number of international organisations suggests proscription has had limited deterrence.

This then raises the issue of proscription interfering with ECHR Article 10 freedom of expression and ECHR Article 11 freedom of assembly and association. In *Attorney General's Reference (No 4 of 2002)*, it was considered that Section 11 (1) TA 2000 interfered with the right to freedom of expression but was necessary and proportionate.[144] In proscribing an organisation under Section 3(4) of TA 2000 the Secretary of State may only exercise his power against named organisations if he believes the organisation is involved in terrorist activities. By Section 3 (5) of TA 2000 an organisation is not only concerned in terrorism by acts of terrorism it commits or participates in, or where it promotes or encourages terrorism, but also where it is 'otherwise concerned in terrorism'. The case of *Secretary of State for the Home Department v Lord Alton of Liverpool*[145] considered the extent to which an organisation can be said to be 'otherwise concerned in terrorism' under section 3(5)(d) of TA 2000 for the purposes of proscription.[146] The Home Secretary proscribed the People's Mojahadeen Organisation of Iran in spite of no evidence of the organisation presenting a specific threat.[147] Proscription has also been applied to support the international community in the 'War on Terror', as evidenced with the recent proscription of al-Shabaab.[148] In this case the government's argument that Section 3(5)(d) TA 2000 continued to apply to an inactive organisation with a history of activity[149] was rejected on the grounds that merely an intention to take up arms in the future is not 'otherwise concerned in terrorism'.[150] The limit of the legislation therefore is that proscription cannot apply to those organisations without military capability and not taking active steps to engage in terrorist acts.[151] This questions the extent to which the government can justifiably interfere with the rights of free speech, assembly and association.[152] The aforementioned affirmation that proscription requires a nexus between an organisation and terrorism and expressing an intention is insufficient, calls into question recent proscription and its proportionality.

Freezing of financial assets also raises the question of the proportionate use of executive power. This was evident in *A v HM Treasury and Others*[153] where in dispute were Orders[154] made under section 1 of the United Nations Act 1946 as appeared 'necessary or expedient' to give effect to Security Council Resolutions 1373 and 1452. The justification for making the orders was to prevent and suppress the financing of terrorist acts and take measures against Al-Qaida. Her Majesty's Treasury used section 1 of the United Nations Act 1946 to make the appellants subject to directions freezing financial assets and criminalising any financial transaction.[155] The UK Supreme Court noted that this system supplanted the existing scheme under Part 2 of ACTSA 2001 with a more draconian system.[156] The UK Supreme Court held this to be an affront to basic rights,[157] because the words 'necessary or expedient' do not permit disproportionate interference with individual rights.[158] There is no parallel with other jurisdictions to this use of executive measures via secondary legislation

[137] N Rasiah, Reviewing Proscription Under The Terrorism Act 2000, (2008) 13 (3) Judicial Review p. 187, para. 2.
[138] C Walker, Blackstone's Guide to The Anti-Terrorism Legislation (2nd edn Oxford University Press 2009) p. 53 para. 2.43.
[139] Lord Carlile, 'Report on the Operation in 2008 of the Terrorism Act 2000 and of Part 1 of the Terrorism Act 2006' (London The Stationery Office 2009) p. 12 para. 50 – 51 http://security.homeoffice.gov.uk/news-publications/publication-search/legislation/terrorism-act-2000/independent-review-responses/Lord-Carlile-report-09?view=Binary accessed 03 May 2010.
[140] B Dickson, Law versus terrorism: can law win?, (2005) 1 European Human Rights Law Review 11 p.p.16 – 17.
[141] SI 2010 No. 34; Hansard 20 January 2010 Security and Counterterrorism 999 – 1000 Lord Strathclyde http://www.publications.parliament.uk/pa/ld200910/ldhansrd/text/100120-0002.htm#10012064000394 accessed 03 May 2010.
[142] Supra note 22, Table 1.10 (a).
[143] Lord Carlile, 'Fifth Report Of The Independent Reviewer Pursuant To Section 14 (3) Of The Prevention Of Terrorism Act 2005' (London The Stationery Office 2010) p. 12.
[144] 2005] 1 Cr App R 28 paragraph 54.
[145] [2008] EWCA Civ 443.
[146] N Rasiah, Reviewing Proscription Under The Terrorism Act 2000, (2008) 13 (3) Judicial Review p. 190 para. 21.
[147] Secretary of State for the Home Department v Lord Alton of Liverpool [2008] EWCA Civ 443 para. 12.
[148] SI 2010 No. 611. House of Commons Hansard Debates for 04 March 2010 David Hanson Column 1035 and 1036 http://www.publications.parliament.uk/pa/cm200910/cmhansrd/chan50.pdf accessed 03 May 2010.
[149] Secretary of State for the Home Department v Lord Alton of Liverpool [2008] EWCA Civ 443 para. 29.
[150] Ibid, para. 127 – 128.
[151] Ibid, para. 37 – 39.
[152] Supra note 147, p. 190, para. 18.
[153] [2010] UKSC 2.
[154] Terrorism (United Nations Measures) Order 2006 SI 2006/2657, Al-Qaida and Taliban (United Nations Measures) Order 2006 SI 2006/2952.
[155] [2010] UKSC 2 at paragraph 38.
[156] [2010] UKSC 2 at paragraph 5 per Lord Hope.
[157] [2010] UKSC 2, para. 45.
[158] Ibid, para. 47.

to target terrorism.[159] The restoration of the domestic asset freezing regime by subsequent emergency legislation [160] and the publication of the draft Terrorist Asset-Freezing Bill which by clause 2 replicates the Treasury power to designate on a reasonable suspicion test and repeats the previous rationale of giving the Treasury power to implement international obligations[161] shows that the UK strategy is entrenched. The justification for this is worded in the CONTEST 2010 annual report as a commitment to the maintenance of 'an effective and proportionate asset regime'.[162] Yet the Supreme Court not only commented on the proportionality of using section 1 (1) of the 1946 Act, but also on the directions under the invalid Orders.

The use of executive measures has become an ingrained practice which is beginning to be challenged in the UK courts on the grounds of proportionality. The Human Rights implications of the implementation of the UK strategy are broader than the question of how proportionate measures are. Proscription becomes difficult to justify where there are no active steps by an organisation to engage in terrorist acts. Nonetheless proscription has been used against organisations on the periphery of terrorist activity and this is a potential threat to free speech, assembly, and association. The use of secondary legislation to freeze financial assets is without precedent and yet the curbing of this by the UK Supreme Court led to emergency legislation designed to reinstate the power.

Legislative Measures of the National Security Strategy

Detention of terrorist suspects before charge illustrates the difficulty of balancing human rights and the requirement of the executive for the greatest power available in the event of an emergency. After the House of Lords rejected the proposed 42-day period for detention without charge in the counter-terrorism bill, the government produced a draft emergency bill[163] with the idea that this could become law in the event of emergency.[164] The UK Parliament Joint Committee on Human Rights urged the government to withdraw this bill on the grounds that legislation rushed through in an emergency receives less scrutiny and enactment could breach ECHR Article 5 rights.[165] On the existing 28-day detention power, concern was repeated about the adequacy of procedural safeguards for authorisation of extended detention.[166] The continued debate is illuminating. In discussing the alternative to pre-charge detention the Joint Committee pointed out that with the increased range of terrorism offences those on the periphery are being arrested.[167] As this implies, the label 'terrorist suspect' makes the anti-terrorism strategy inflexible.[168]

The underlying purpose of pre-charge detention becomes apparent when considering the government case for a 90-day period. The evidence before the Home Affairs Committee was that the purpose of early arrest is to disrupt conspiracies in the interests of public safety.[169] Labelled 'preventative detention' this is the real driver for extended detention.[170] This may explain why arguments for alternatives such as bail, charging on a threshold test of reasonable suspicion of a criminal offence having been committed, and the use of intercept evidence, has not changed the government's insistence on the need for extended powers of detention without charge. An audit of rights commented on an emerging 'shadow system of criminal justice' controlled by the executive.[171]

'Operation Pathway' reported on by Lord Carlile demonstrates the shortcomings of the argument for 'preventative detention'.[172] Although the initial applications for warrants of further detention were granted[173], the UK High Court said further application would have to show a "real prospect of evidence".[174] The finding that nothing of value was obtained during detention is not an isolated case.[175] In the 'airline liquid

---

[159] Ibid, para. 50 – 53.

[160] The Terrorist Asset-Freezing (Temporary Provisions) Act 2010 In Force 10 February 2010 – 31 December 2010.

[161] 'Publication in draft of the Terrorist Asset-Freezing Bill' Cm 7806 February 2010 Explanatory notes paragraph 8, http://www.hm-treasury.gov.uk/d/finsanc_assetfreezingbill_draft_050210.pdf accessed 14 April 2010.

[162] Supra note 62, p. 10 para. 2.12.

[163] Counter-Terrorism(Temporary Provisions)Bill, www.parliament.uk/deposits/depositedpapers/2008/DEP2008-2775.pdf accessed 15 April 2010.

[164] http://www.telegraph.co.uk/news/newstopics/politics/lawandorder/3192152/Jacqui-Smith-creates-emergency-bill-after-42-day-detention-defeat.html accessed 15 April 2010.

[165] Joint Committee on Human Rights, 'Counter-Terrorism Policy and Human Rights (Seventeenth Report): Bringing Human Rights Back In [16th Report Session 2009-10] HL 86 HC 111, p. 29 para. 82 – 83 http://www.publications.parliament.uk/pa/jt200910/jtselect/jtrights/86/86.pdf accessed 15 April 2010.

[166] Ibid, p. 26, para. 69 – 70.

[167] Joint Committee on Human Rights, 'Counter-Terrorism Policy and Human Rights (Sixteenth Report): Annual Renewal of Control Orders Legislation 2010 [9th Report Session 2009-10] HL 64 HC 395. http://www.publications.parliament.uk/pa/jt200910/jtselect/jtrights/64/64.pdf accessed 11 April 2010.p. 30 , para. 88.

[168] S Greer, Human Rights and the Struggle Against Terrorism in the United Kingdom, (2008) 2 European Human Rights Law Review 163, p. 169.

[169] Home Affairs Committee, 'Terrorism Detention Powers' Fourth Report [Session 2005- 06] HC (2006) 910-1 p. 30 para. 91 – 93, http://www.publications.parliament.uk/pa/cm200506/cmselect/cmhaff/910/910i.pdf accessed 16 April 2010.

[170] Ibid, p.p. 30 – 31 para. 94 – 95.

[171] A Blick and T Choudhury and S Weir, The Rules of the Game Terrorism Community and Human Rights, (The Joseph Rowntree Reform Trust 2006) , p. 48 http://www.jrrt.org.uk/uploads/Terrorism_final.pdf accessed 16 April 2010.

[172] Lord Carlile, Operation Pathway Report Following Review (October 2009) http://security.homeoffice.gov.uk/news-publications/publication-search/legislation/terrorism-act-2000/operation-pathway-report?view=Binary accessed 16 April 2010.

[173] Lord Carlile, 'Fifth Report Of The Independent Reviewer Pursuant To Section 14 (3) Of The Prevention Of Terrorism Act 2005' (London The Stationery Office 2010) paragraph 79.

[174] Ibid, para. 80.

[175] Ibid, para. 88.

bomb case' the main protagonists were charged within 14 days of detention whilst those detained up to the 28-day limit were either not charged or were subsequently acquitted. The implication was that pre-charge detention operates unfairly against those on the periphery.[176] This exposes a Human Rights deficit in the anti-terrorism strategy. As distinct from non-terrorist investigations early arrest will be on a threshold basis of reasonable suspicion of terrorism offences, where for example the full extent of a conspiracy is unknown and the full evidence is yet to emerge. As Lord Carlile points out a Section 41 TA 2000, arrest is unique in terms being a terrorist is not a criminal offence.[177] As compliance with ECHR Article 5 is by judicial scrutiny in each case of whether there is justification for further detention the argument for extended detention for a preventative purpose cannot be justified.[178]

The use of legislative measures for a preventative purpose and intervention at an earlier stage in terrorist plots is shown by the UK development of anticipatory offences. Sections 1 to 3 of the TA 2006 are part of the preventive strategy against the expression of terrorism, the intention being to create a permanent legislative framework for 'addressing terrorism' as opposed to responding to it.[179]

It is acknowledged that section 1 TA 2006 encouragement of terrorism offence is controversial.[180] However, Lord Carlile's view was that section 1 did not criminalise 'mere preaching'.[181] As developments now show, criminalising encouragement of terrorism facilitates suppression of extremist views without prosecution for criminal offences. Where material published on the internet relates to encouragement of terrorism or dissemination, Section 3 TA 2006 applies to give police the power to either require the removal of internet material or modification of its content.[182] On February 1st, 2010 the Home Office launched an online scheme for the public to report terrorist material to a police team investigating extremist sites with the intention police will use these powers.[183] This is a strategy to prevent people becoming influenced by terrorism. Indeed, when the 2006 Act was in its draft stage and was put to the Home Secretary his response was that the purpose was to make it more difficult for people susceptible to preaching to 'transition' to undertaking terrorist acts.[184] This illustrates anti-terrorist legislation has a counter-terrorist purpose.

Arguably, the encouragement offence can criminalise 'mere preaching'. The offence includes not only encouragement but 'other inducement' and therefore applies not only to express or implied statements of encouragement.[185] As section 1 (5) TA 2006 makes it irrelevant whether encouragement relates to either particular acts or particular Convention offences and whether anyone was induced or encouraged, and includes past and future glorification[186], the offence is capable of including any expression construed as the encouragement of terrorism.[187] Furthermore, the definition of 'acts of terrorism' which are encouraged by section 20 TA 2006 includes anything within the meaning of section 1 (5) of TA 2000. Section 1(5) defines an act of terrorism as an act or 'threat of action' with the purpose of not only to influence the government but also to intimidate a section of the public for the advancement of a political, religious or ideological cause.[188] Because of this the encouragement offence can be argued to catch all forms of protest at the detriment to freedom of expression.[189] Since the Counter-Terrorism Act 2008 widened the definition of terrorist purpose to include racial[190] – thereby widening the encouragement offence – this shows the implementation of anti-terrorism strategy targeting all extremism can be readily achieved by amending the definition of terrorism.[191] The role of the legal definition of terrorism in expanding offences is part of the early interventionist strategy.[192] This challenges legal certainty and leaves scope for confusion as to when views sympathetic to terrorism amount to encouragement.[193]

Criminalising the dissemination of terrorist publications is equally wide as this includes the possession of a publication with a view to dissemination [194] and recklessness will suffice.[195] In *Bilal Mohammed* his reckless sale of material amounting to a terrorist publication drew the distinction between his case and that of a dedicated extremist seeking to encourage

[176] A N Bajwa and B O'Reilly, Public/Human Rights: Terrorising the Innocent, (2010) 160 New Law Journal, p. 481.

[177] Lord Carlile, 'Fifth Report Of The Independent Reviewer Pursuant To Section 14 (3) Of The Prevention Of Terrorism Act 2005' (London The Stationery Office 2010) , para. 60.

[178] R (on the application of I) v Westminster Magistrates Court [2008] EWHC 2146 (Admin) at para. 21 – 23.

[179] Hansard Commons Draft Terrorism Bill Minutes of Evidence HC 515-i 11 October 2005 Q2 Rt Hon Charles Clark MP http://www.publications.parliament.uk/pa/cm200506/cmselect/cmhaff/515/5101102.htm accessed 18 April 2010.

[180] Lord Carlile, 'The Definition of Terrorism' (Cm 7052 Norwich The Stationery Office March 2007) , p. 38 para. 68.

[181] Ibid, p.p.40 – 41 para. 72.

[182] Section 3 (3) Terrorism Act 2006.

[183] Press Release, 'Public reporting mechanism for terrorist material on the internet' 01 February 2010 http://press.homeoffice.gov.uk/press-releases/public-reporting-terrorist accessed 17 April 2010.

[184] Hansard Commons Draft Terrorism Bill Minutes of Evidence HC 515-i 11 October 2005 Q3 Rt Hon Charles Clark MP http://www.publications.parliament.uk/pa/cm200506/cmselect/cmhaff/515/5101102.htm accessed 18 April 2010.

[185] Section 1 (1) Terrorism Act 2006.

[186] Section 1 (3) Terrorism Act 2006.

[187] A Hunt, Criminal Prohibitions on Direct and Indirect Encouragement of Terrorism, (2007) Crim LR (6) 441, p. 448 and I Ward, God, Terror and Law, (2008) 28 (4) Oxford Journal of Legal Studies 783, p. 788.

[188] Section 1 (1) (a) (b) (c) Terrorism Act 2000.

[189] D McKeever, The Human Rights Act and Anti-terrorism in the UK: One Great Leap Forward By Parliament, But Are The Courts Able To Slow The Steady Retreat That Has Followed?, (2010) Jan Public Law 110, p. 128.

[190] Section 75 (1) (2) (a) Counter-Terrorism Act 2008.

[191] Supra note 190, p. 116.

[192] C Walker, Blackstone's Guide to The Anti-Terrorism Legislation (2nd edn Oxford University Press 2009) p. 8 para. 1.24.

[193] Supra note 188, p.p. 449 – 450.

[194] Terrorism Act 2006 section 2 (2) (f).

[195] Terrorism Act 2006 section 2 (1) (c).

terrorist activity.[196] The significance of this, as pointed out by Ramage, is that people who have no proven link to terrorism can be prosecuted on the basis that their acts create a remote risk of harm.[197] This is noted in the distinction Hunt draws between the dissemination offence and incitement, in that the possessor of a terrorist publication need have no direct involvement in encouraging terrorism.[198]

All the aforementioned measures go beyond the Council of Europe Convention on the Prevention of Terrorism (CEPT) obligations to take effective measures to prevent terrorism.[199] Under Article 5 (1) of the CEPT, public provocation requires 'intent to incite' a terrorist offence and a casual connection between publication and a danger that offences may be committed. Like the CEPT, the international obligation is also to prevent incitement and to show causal connection.[200] Whilst Article 19 of the International Covenant on Civil and Political Rights permits restriction to freedom of expression and the ECHR Article 10 right is a qualified right, the removal of the conditions of incitement and harm reduces protection.

The UK Parliament Joint Committee on Human Rights identified that section 1 of the TA 2006 was wider than Article 5 CEPT[201], risking making this incompatible with the ECHR Article 10 right.[202] The fundamental criticism of the encouragement offence was the "chilling effect" of the offence preventing people voicing their views[203] leading to disproportionate interference with free speech.[204] As reviewed by the International Commission of Jurists, States including the UK have gone beyond international obligations to prevent incitement.[205] The UK indirect encouragement provision was cited as one of the most controversial examples of this.[206] The real danger is that the use of anti-terrorism legislation is no longer perceived to be legitimate but instead victimises people for their views.[207] The UK role in the 'War on Terror' having emphasised preventative measures as a key part of the anti-terrorism strategy has created legislation capable of being used not only to prevent terrorism but suppress views. This is a threat to the ECHR Article 10 right to freedom of expression.

But this development of the UK strategy appears to be in keeping with what the Council of Europe has encouraged EU Member States to adopt. For example, the Council of Europe in 2008 modified its 2002 Framework Decision on combating terrorism, which is the basis of the counter-terrorist policy of the European Union.[208] The 2008 amendment by the Council of Europe requires EU Member States to criminalise acts linked to terrorist activities, particularly by taking action against the publication and dissemination of materials capable of inciting people to commit acts of terrorism. In turn, this is justified in accordance with international law obligations under United Nations Security Council Resolution 1624 (2005) in order to prevent incitement to commit terrorist acts.[209] The amendment to the Framework decision is considered an important step towards targeting the use of the internet to incite terrorism.[210]

Recent case law suggests freedom of expression is becoming eroded by a general approach of asking what is in the interests of national security. For example in the context of glorifying terrorism offences, Sottiaux criticised the recent ECHR decision of *Leroy v France*[211] as moving away from traditional incitement law[212] to deciding- as in this case- whether Mr Leroy's cartoon of the World Trade Centre twin towers could be interpreted as glorifying violence despite his intention to simply express Anti-Americanism.[213]

The UK Strategy goes beyond targeting the organisers of terrorist training. Whereas section 6 TA 2006 reflects Article 7 of the CEPT in criminalising training for terrorism[214], Section 8 goes further to criminalise attendance at places used for terrorist training. The UK Court of Appeal case of *R v Da Costa and Others*[215] considered the construction of the two sections. Whilst the test in Section 6 (1) (b) is that the provider knows an attendee's intention to use his training for terrorist purposes[216], for the Section 8 offence it is sufficient that the training is given for

[196] Abdul Rahman and Bilal Mohammed [2008] EWCA Crim 1465 at para. 34 – 37.
[197] S Ramage, The Little Red School Book and Other Harmful Publications, (2008) 186 Criminal Lawyer 1
[198] Supra note 188 , p. 445.
[199] Council of Europe Convention on the Prevention of Terrorism CETS No 196 http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=196&CM=1&CL=ENG accessed 03 May 2010.
[200] UN Security Council Resolution 1624 (2005) adopted 14 September 2005 UN Doc S/RES/1624 (2005).
[201] Joint Committee on Human Rights, 'The Council of Europe Convention on the Prevention of Terrorism' [1st Report Session 2006-07] HL 26 HC 247, para. 22 – 39, http://www.publications.parliament.uk/pa/jt200607/jtselect/jtrights/26/26.pdf accessed 17 April 2010.
[202] Ibid, para. 29.
[203] Ibid, para. 40 – 49.
[204] Ibid, para. 47.
[205] International Commission of Jurists, 'Assessing Damage, Urging Action: Report of the Eminent Jurists Panel on Terrorism, Counter-terrorism and Human Rights' (Geneva 2009), p.p. 127 – 128.
[206] Ibid, p.p. 129 – 130.
[207] C Walker, Clamping Down on Terrorism in the United Kingdom, (2006) 4 (5) Journal of International Criminal Justice 1137, p. 1141.
[208] 'Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism' Official Journal of the European Union L 330/21 para. (2).
[209] Ibid, .para. 7 and 8.
[210] MEMO/08/255 Amendment of the Framework Decision on combating terrorism Brussels 18 April 2008 http://www.libertysecurity.org/article2010.html accessed 21 April 2010.
[211] 36109/03 Unreported October 2 2008 ECHR.
[212] S Sottiaux, Leroy v France: Apology of Terrorism and the Malaise of the European Court of Human Rights, Free Speech Jurisprudence' (2009) 3 European Human Rights Law Review 415, p. p. 417 - 420.
[213] Supra note 211, p.p. 420 – 422.
[214] Council of Europe Convention on the Prevention of Terrorism CETS No 196 http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=196&CM=1&CL=ENG accessed 03 May 2010.
[215] [2009] EWCA Crim 482
[216] R v Da Costa and Others[2009] EWCA Crim 482 at para. 15.

terrorist purposes.[217] Since an attendee can commit an offence on a lesser test of belief or lack of reasonable belief[218] and does not need an intention to put the training to use[219] or otherwise can commit the offence without undergoing training[220], criminal liability is much wider for those that take part than for the promoters and organisers of terrorist training.

This extended reach of the legislation in the anti-terrorism strategy is illustrated by the possession offences. The UK Court of Appeal in *R v Malik*[221] observed that where material is downloaded from the internet with the intention to be used to assist acts of terrorism the section 58 TA 2000 offence of the collection of information could be committed.[222] This could be the case even if intention is subsequently abandoned and it implies that mere possession could suffice. Indeed in *R v G*[223] the UK House of Lords confirmed that as section 58 is concerned with the 'nature of the information' possessed, then the purpose for collecting information is irrelevant. Recently in *R v Muhammed (Sultan)*[224], the UK Court of Appeal held that section 58 TA 2000 is not to be narrowly interpreted so as to be only limited to furthering the actual commission or preparation of terrorist acts. It was held that it is impractical to distinguish between the stages of preparation required for a document or record to become useful to a person committing or preparing an act.[225] Absent reasonable excuse, this has wide application to those who possess material for non-terrorist purposes.

Therefore, the strategy disproportionately targets those on the periphery, fantasists as opposed to terrorists.[226] This is facilitated by the difference of protective intention tests applied to genuine terrorists and those on the periphery. By the nature of the offences they are charged with, the former are subject to less protection where specific intention and connected purpose are absent, a difference the courts have reinforced.

The UK, whilst acting in accordance with international obligations and European policy, has made the legislative measures capable of wide use against those on the periphery of terrorism. In doing so, it has not addressed the issue of how to safeguard rights. The real threat becomes that anyone in possession of material deemed to be for a terrorist purpose regardless of their intent is capable of being targeted under the anti-terrorism legislation. This shows how the implementation of the strategy again affects rights of freedom of expression, assembly and association. It is not only the promoters and organisers of terrorism the strategy is able to target. Its far reaching nature carries the implication that there has been a noticeable shift away from targeting terrorists and terrorism. This defines a new era in the 'War on Terror' where the emphasis is no longer on terrorist conflict but on using criminal justice to prevent terrorism. Pre-charge detention is used to make early arrests in the interests of disrupting terrorist activity. The implication is that the executive controls criminal justice at the expense of the ECHR Article 5 right to liberty. Anticipatory offences created under TA 2006 have created a legislative framework designed to enhance the prevention of terrorism. The ability to use this legislation to silence expression of extremist views particularly illustrates the use of anti-terrorism legislation as a mechanism of control. The problem is acute once the definition of terrorism is widened. Then any extremist view can be targeted, threatening to stifle freedom of expression.

Arbitrary Use of Anti-Terrorism Powers in the United Kingdom

In practice there is a risk of the arbitrary use of power. On available evidence the Section 44 TA 2000, stop and search power is of questionable value beyond deterrent effect especially where the number of police searches is out of proportion to arrests.[227] Section 44 (2) TA 2000 gives a police constable in uniform authorisation to stop and search a pedestrian. The authorisation can cover an area of place and can be the whole or part of a police area. The requirement in section 44 (3) TA 2000 is that authorisation may be given by a senior officer only if considered 'expedient for the prevention of acts of terrorism'. Since 'reasonable suspicion' is not required to use Section 44 TA 2000 to stop and search people, the power can be used against anyone[228] as confirmed by the European Court of Human Rights in *Gillan and Quinton v The United Kingdom*.[229] The finding was that the use of the power amounted to a breach of ECHR Article 8 rights of respect for private life.[230] This was on the grounds that the use of the power was arbitrary because of the broad discretion police officers have in their exercise of the stop and search power once given what amounts to a blanket authority to use the power.[231] The authorisation procedure itself was considered to lack any assessment of proportionality[232] and authorisation continuously renewed on a rolling basis without any scrutiny.[233] This has the following ramification: there has to be control over the risk of arbitrary use to justify interference in ECHR rights. The evidence of the excessive use of the

[217] Section 8 (1) (c) Terrorism Act 2006.
[218] Section 8 (2) (a) (b) Terrorism Act 2006.
[219] R v Da Costa and Others [2009] EWCA Crim 482 at paragraph 21.
[220] Section 8 (3) (a) Terrorism Act 2006.
[221] [2008] EWCA Crim 1450.
[222] R v Malik [2008] EWCA Crim 1450 at paragraph 41.
[223] [2009] UKHL 13; [2010] 1 AC 43 HL.
[224] [2010] EWCA Crim 227.
[225] [2010] EWCA Crim 227 at paragraph 46.
[226] K D Ewing, Bonfire of the liberties New Labour Human Rights and the Rule of Law (Oxford University Press 2010), p. 211.
[227] D Thiel, Policing Terrorism A Review of the Evidence, (The Police Foundation 2009), p. p. 32 – 33.
[228] Ibid, p.p. 32 – 33.
[229] [2009] ECHR 28 12 January 2010 Application no 4158/05
[230] Ibid, para. 87.
[231] ibid, para. 85.
[232] Ibid, para. 80.
[233] Ibid, para. 81 – 82.

power[234] demonstrates that the UK anti-terrorism strategy is too reliant on discretion.[235]

Counter-terrorism Measures in the United Kingdom and the 'War on Terror'

Compared to the US conceptualisation of the 'War on Terror' as a military response[236], Europe takes a long-term view of addressing underlying causes[237] with the focus on investigation and prevention.[238] As seen the UK aligns to this EU model and vice versa. However, post-9/11, the UK role has interpreted international obligations to use anti-terrorism legislation[239] for deterrence purposes remodelling domestic criminal law to aggressively target terrorism as opposed to terrorists.[240] It is the pre-emptive aspect of the strategy that has created new laws targeting an ever greater range of people and activities[241] embedding national security into the criminal justice system.[242] This creates a new paradigm for the 'war on terrorism'. As seen human rights compliance is becoming questionable.

To use the terminology 'War on Terror' is to suggest action is being taken against armed conflict and therefore International Humanitarian Law (IHL) rules applying to armed conflict become applicable. As Duffy identifies, the terminology can be a pretext to use IHL to justify the detention of terrorists on the grounds of enemy combatants and whether such steps are taken the danger is the ambiguities surrounding the loose use of terminology enable States to manipulate the law.[243] But the UK anti-terrorism strategy does not justify the use of this terminology. Having taken the stance that terrorism is a threat to be managed and the risk of terrorism can be reduced by appropriate measures, the UK strategy is not prosecuting a war on terror but devising measures for controlling terrorism. This demands higher standards of legal protection to those affected by the measures. As Walker identified the UK terrorism legislation follows the criminal justice model and not a war model. This has clear implications for detention without trial and the application of control orders.[244] His argument is that extraordinary measures should be made subject to derogation and instead alternatives should be found.[245] As seen with the continued use of control orders despite the government identifying that international terrorism is not a strategic threat to the UK, the use of extraordinary measures are becoming a permanent feature of the UK anti-terrorism strategy. With the emphasis now on pre-emptive measures and the paradox of a legislative system where people committing anticipatory offences are less protected by the law (and more easily prosecuted) the implications are that liberty (whether of person or expression) is becoming reduced to the question of what is in the best interests of national security.

The counter-productive effects of this are suggested by Campbell and Connolly using Northern Ireland as an object lesson.[246] They talk of a 'grey zone' of executive power created by anti-terrorist law[247], which moves beyond law however much cloaked with legislative authority[248] creating a new species of violent opposition, thereby sustaining terrorism.[249] They cite the use of the anti-terrorist stop and search powers in the UK as evidence of indiscriminate use capable of alienating British Muslims.[250] The impact of the UK anti-terrorism legislation post 9/11 is to make all Muslims potential terrorist suspects.[251] The negative aspect of the 'war on terrorism' is this divisiveness[252] as demonstrated by for example proscription[253] and reinforced by discretionary powers within the TA 2000.[254] This results in a dual criminal justice system with an extraordinary sphere directed not at prosecution but at pre-empting terrorism.[255] It is the pre-emptive aspect of the strategy that has created new laws targeting an ever greater range of people and activities before terrorist acts have been committed[256] embedding national security into an anti-terrorism criminal justice system.[257] It remains to be seen whether this is positive or negative in the long-term. Arguably the UK contribution has been to develop the concept of pre-emption in the domestic law sphere thereby creating a new paradigm for the 'War on Terrorism'.

The implementation of the strategy therefore creates the very conditions for radicalisation the strategy seeks to avoid.[258] Whilst the strengths of the UK strategy

[234] Ibid, para. 84.
[235] R Edwards, Stop and Search, Terrorism and the Human Rights Deficit, (2008) 37 (3) Common Law World Review 211, p.p. 223 – 230.
[236] H Duffy, The 'War on Terror' and the Framework of International Law (Cambridge University Press 2005), p. 123.
[237] D Keohane, The Absent Friend: EU Foreign Policy and Counter-Terrorism, (2008) 46 (1) Journal Common Market Studies 125, p.p. 134 – 135.
[238] M Lehto, War on Terror – Armed Conflict With Al-Qaida? (2010) 78 Nordic Journal of International Law 499, p.p. 502 - 503.
[239] B Brandon, Terrorism, Human Rights and the Rule of Law: 120 Years of the UK's Legal Response to Terrorism (2004) Crim LR 981 p. 996.
[240] D Whittaker, Counter-Terrorism and Human Rights (Pearson Education Limited 2009).
[241] J McCulloch and S Pickering, Pre-Crime and Counter-Terrorism: Imagining Future Crime in the "War on Terror" (2009) 49 (5) British Journal of Criminology 628 p. 633.
[242] Ibid, p.p.634 – 640.
[243] Supra note 247, p.p. 271 – 272.
[244] Supra note 208.
[245] Ibid.
[246] C Campbell and I Connolly, Making War on Terror? Global Lessons from Northern Ireland (2006) 69 (6) Modern Law Review 935, p. 937.
[247] Ibid, p.943.
[248] Ibid, p. 944.
[249] Ibid, p.p. 954 – 956.
[250] Ibid, p.p.956 – 957.
[251] C Pantazis and S Pemberton, From the "Old to the "New" Suspect Community: Examining the Impacts of Recent UK Counter-Terrorist Legislation (2009) 49 (5) British Journal of Criminology p. 646.
[252] Ibid, p.p. 650 – 651.
[253] Ibid, p. 652.
[254] Ibid, .p. 653.
[255] Ibid, .p. 654.
[256] J McCulloch and S Pickering, Pre-Crime and Counter-Terrorism: Imagining Future Crime in the "War on Terror (2009) 49 (5) British Journal of Criminology 628, p. 633.
[257] ibid, p.p. 634 – 640.
[258] Ibid, p. 661.

lie in the security values of controlling terrorism and as such this aligns with United States and European policies, the weaknesses are the disproportionate use of anti-terrorism legislation against non-terrorists and the primacy of executive control. This undermines the legitimacy of continuing with the strategy and limits public confidence. The effect of using anti-terrorism legislation to include targeting would-be terrorists or people who express support for a terrorist cause may restrict the rights of liberty and freedom of expression. This makes those Human Rights subordinate to the interests of National Security.

Conclusion

Anti-terrorist legislation has a counter-terrorism purpose and counter-terrorist policy is driving the evolution of anti-terrorism strategy. This is reflected in the development of anticipatory offences and is clear from the expression of the strategy as an overarching counter-terrorism national security strategy. A hybridisation of the criminal justice model can be detected from the increasing use of executive power. This is reflected in control orders, proscription and the use of financial restraint. In effect there is legal ground lying between the criminal justice model and the war model. Whilst the UK does not have a 'homeland security' model comparable to the United States, the UK model can be defined as a national security model in which anti-terrorism legislation has the lead role. This has clear implications for human rights as they are in danger of becoming offset as opposed to being an equal interplay of liberty and security. The implications of the emerging imbalance are the UK long-term contribution to the 'War on Terror' could be the furtherance of extremism as an unintended consequence.

Creating More Turmoil: Why UAV strikes Will Be Counterproductive in Yemen

William Mayborn

Introduction:

This paper seeks to answer the question of whether the U.S. should expand the use of Unmanned Aerial Vehicles (UAVs) to execute targeted killings in Yemen. This is an important question for two reasons: 1) al Qaeda affiliates use Yemen as a safe haven for planning and executing terrorist operations, and 2) the current political upheaval in Tunisia, Libiya and Egypt is encouraging further demonstrations and protests in Yemen. To answer the UAV expansion question this paper will examine political instability issues in Yemen, recent Yemeni terrorist activities, current U.S. policy towards Yemen, previous use of a Predator drone in Yemen, and ways to improve Yemen-U.S. counter-terrorism cooperation.

Yemen Instability and Governance Issues:

Yemeni internal political discord continues to hamper the development of the nation as it contends with two secessionist insurgencies: the Northwest al Houthi insurgency[1] (also referred to as the Believing Youth, or Shabab al Moumineen),[2] and the comparatively less contentious Southern insurgency.[3] Yemeni President Ali Abdallah Salih's insurgent difficulties compound the terrorist problem because insurgent-held areas offer operational space to terrorist groups.

Since 2004, the Yemen and Saudi Arabian governments have tried to link the al Houthi insurgents to al Qaeda in an attempt to garner international approval of their military focused counter insurgency methods. Saudi Arabian warplanes attacked al Houthi positions inside Yemen on November 5, 2010; Saudi Arabia's first cross border military intervention since 1991 when they participated in the Gulf War.[4] Al Houthi insurgents do express disdainful rhetoric against Saudi and U.S. governments because both support their opposition, the Yemen government, but the al Houthi insurgents have not attacked Westerners to date. They focus their ambushes, sniper attacks, and small to medium sized bombs on the Yemini army and police forces.[5]

Aside from the two insurgencies, the Yemeni government is facing dire social, political, and economic challenges: an illiteracy rate greater than 50%, half the population earns less than $2 a day, and 75% of state revenues come from oil resources that are predicted to run dry by 2017.[6] With a population of 23.4 million,[7] Yemen has an estimated 250,000 refugees from the al Houthi insurgency battles.[8] In comparing global index values, Yemen ranks as one of the worst countries in the areas of Human Development, Failed State, Political Stability, Government Effectiveness, and Rule of Law.[9]

Defense analyst C. C. Brafman Kittner proposes that weak governments that are unable to inhibit weapons proliferation, transnational criminal activities, and drug trafficking are ideal countries for terrorists to find safe havens. She explains that in weak states "the veneer of state sovereignty" still exists and can actually shield the terrorist organizations from international countermeasures.[10] Kittner points to the Yemen situation as an example of a central government's inability to control mountainous border areas inhabited by terrorists and smugglers.[11] In addition, the Yemen border areas are tribal areas outside of the central

---

[1] Office of the Coordinator for Counterterrorism, *Country Reports on Terrorism 2009*, August 5, 2010, U.S. State Department, http://www.state.gov/s/ct/rls/crt/2009/140886.htm, (Nov. 29, 2010).

[2] Jack Freeman, "The al Houthi insurgency in the North of Yemen: An Analysis of the Shabab al Moumineen", *Studies in Conflict and Terrorism,* 2009, p. 1008. http://www.informaworld.com/smpp/content~db=all~content=a916106970~frm=titlelink?words=houthi,insurgency,north,yemen,analysis,shabab,moumineen, (Nov. 3, 2010).

[3] Agence France Presse *18 killed in south Yemen violence this year: report*, April 17, 2010, Google News, http://www.google.com/hostednews/afp/article/ALeqM5gpQHbHPPIGbgzBxShvlEhgwurgLw, (Dec. 7, 2010).

[4] Joost R. Hiltermann, "Disorder on the Border", *Foreign Affairs*, December 16, 2009, http://www.foreignaffairs.com/articles/65730/joost-r-hiltermann/disorder-on-the-border, (Nov. 3, 2010).

[5] Freeman, p. 1013.

[6] U.S. Senate Committee on Foreign Relations, *Al Qaeda in Yemen and Somalia: A Ticking Time Bomb,* January 21, 2010, U.S. Government Printing Office, pp. 8-9, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_senate_committee_prints&docid=f:54494.pdf, (Dec. 6, 2010).
Other estimates state that the oil reserves will expire by 2020 to 2030, see *Yemen on the Brink: Implications for U.S. Policy*, p. 14.

[7] CIA- The World Factbook, *Yemen,* Central Intelligence Agency, https://www.cia.gov/library/publications/the-world-factbook/geos/ym.html, (Dec. 9, 2010).

[8] House of Representatives, Committee on Foreign Affairs, *Yemen on the Brink: Implications for U.S. Policy*, February 3, 2010, U.S. Government Printing Office, p. 10. http://permanent.access.gpo.gov/lps123153/54939.pdf, (Dec. 6, 2010).

[9] Edward Newman, "Weak States, State Failure and Terrorism", *Terrorism and Political Violence,* 2010, p. 480, http://www.informaworld.com/smpp/content~db=all~content=a783497486~tab=content~order=page, (Nov. 3, 2010).

[10] Cristiana C. Brafman Kittner, "The Role of Safe Havens in Islamist Terrorism", *Terrorism and Political Violence*, 2007, p. 310, http://www.informaworld.com/smpp/content~db=all~content=a780502437~frm=titlelink?words=role,safe,havens,islamist,terrorism (Nov. 3, 2010).

[11] Kittner, p. 309. Kittner makes an interesting observation that honey smuggling from Yemen into Saudi Arabia is a lucrative trade for terrorists, and the honey containers are often considered "too messy" for the custom inspectors. Thus, honey containers are perfect for concealing drugs, arms, gold, electronic equipment and cash.

government's authority, and they often offer hospitality to Islamist terrorists.[12]

In January 2011, Secretary of State Hillary Clinton visited Yemen and expressed her fears concerning the political fragility of the country. With the recent events in Tunisia and Egypt, the secretary's fears are being realized as demonstrations in southern Yemen and in the capital have increased in fervency.[13] The removal of the current Salih government could lead to further unrest in the country and encourage more Islamist terrorist organizations to seek safe haven in Yemen.

Yemeni Terror Operations:

Yemeni based terrorism came to the forefront of U.S. attention when the U.S.S. Cole was attacked on October 12, 2000 killing 17 U.S. Navy personnel, and wounding 39.[14] The nation experienced a "brief period of calm" due to successful negotiations between the Yemen government and extremists, and improved U.S.-Yemeni counter-terrorism cooperation.[15] However, after 2004, Al Qaeda and Sunni Islamists in Yemen reacted to the U.S. invasion of Iraq by attacking Western targets and Yemen security targets.[16] The most notable attack was on the U.S. Embassy in Sana'a on September 17, 2008 killing eleven Yemeni civilian security personnel. The U.S. State Department responded by evacuating all nonessential personnel from the Sana'a embassy.[17]

The terrorist threat in Yemen became increasingly adverse in January 2009 when al Qaeda Yemen (AQY) and Al Qaeda elements in Saudi Arabia merged to form al Qaeda in the Arabian Peninsula (AQAP). After the creation of AQAP there was an increase in terrorist planning and recruitment for operations in Saudi Arabia and against foreign nationals in Yemen.[18] The merger has also produced an increase in attempts to bomb U.S. domestic targets from Yemen: for example, the Christmas 2009 "underwear bomber"[19] and the October 2010 printer cartridge bombs.[20] Also, it should be noted that the Fort Hood shooting[21] can be linked to Yemen-based American imam, Anwar al-Awlaki.[22]

Current U.S. Policy:

The U.S. government recognizes that Yemen's insurgent and terrorist security challenges are hindering the social, economic and political development problems; therefore, U.S. foreign policy toward Yemen attempts to be "holistic and flexible."[23] The current policy seeks to accomplish two goals:

> (1) Strengthen the Government of Yemen's ability to promote security and minimize the threat from violent extremists within its borders.
> (2) Mitigate Yemen's economic crisis and deficiencies in government capacity, provision of services, transparency, and adherence to the rule of law.[24]

The U.S. government has sought to help refugees from the al Houthi insurgency with $7.4 million in food aid, $3.1 million in relief aid, and $4.4 million in refugee assistance aid.[25] At present, U.S. military aid is an estimated $155 million to assist Yemen's counter-terrorism efforts by providing helicopters, materials, and U.S. Special Forces trainers.[26] U.S. military leaders plan to increase military aid in 2011 to an estimated $250 million.[27] The U.S. State Department report implies that these counter-terrorism resources led to four successes in 2009:

> (1) January 19, 2009, the Yemen Counter-terrorism Unit raided an AQ cell in the capital city of Sana'a killing two suspects, capturing one suspect and confiscation of a large weapons cache containing machine guns, RPGs and mortars.
> (2) March 2009, successful arrest of a Saudi AQAP member in Ta'iz, Yemen.
> (3) June 2009, successful arrest and surrender of a Saudi AQAP member and a Saudi AQAP financier, Hasan Hessian bin Alwan.

---

[12] Ibid, p. 311.

[13] Nada Bakri and J. David Goodman, "Thousands in Yemen Protest Against the Government," *New York Times,* January 27, 2011, http://www.nytimes.com/2011/01/28/world/middleeast/28yemen.html?_r=1&scp=2&sq=Yemen&st=cse, (Jan. 29, 2011).

[14] Seth G. Jones and Martin C. Libicki, *How terrorist groups end: lessons for countering al Qa'ida,* RAND MG741-1, RAND Corporation, http://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG741-1.pdf, (Nov. 29, 2010) p. 187.

[15] *Al Qaeda in Yemen and Somalia: A Ticking Time Bomb*, p. 11.

[16] Ibid, p. 12.

[17] Ibid, p. 8.

[18] *Country Reports on Terrorism 2009*.
March 15, 2009- Four South Korean tourists were killed in a suicide bomb attack.
March 18, 2009- South Korean government motorcade was attacked by a suicide bomb attack.
June 2009- Nine foreigners were kidnapped in Sa'ada, Yemen: three confirmed deaths, six still missing.

[19] For Underwear bomber details see Steven Erlanger, "Yemen Says Bomb Suspect Met With Qaeda Figures", *New York Times,* January 7, 2010, http://www.nytimes.com/2010/01/08/world/middleeast/08yemen.html, (Dec. 8, 2010).

[20] For Printer cartridge bomb plot details see "Bomb was designed to explode on cargo plane – UK PM", *British Broadcasting Corporation,* October 30, 2010, http://www.bbc.co.uk/news/world-us-canada-11657486, (Dec. 8, 2010).

[21] For Fort Hood shooting details see Elisabeth Bumiller and Scott Shane, "Pentagon Report on Fort Hood Details Failures", *New York Times,* January 15, 2010, http://www.nytimes.com/2010/01/16/us/politics/16hasan.html, (Dec. 8, 2010).

[22] *Al Qaeda in Yemen and Somalia: A Ticking Time Bomb*, p. 9.

[23] *Yemen on the Brink: Implications for U.S. Policy*, p. 10.

[24] Ibid, p. 10.

[25] House of Representatives, Committee on Foreign Affairs, "Yemen on the Brink: Implications for U.S. Policy", p. 10.

[26] Dawn, "US weighs options against militant threat in Yemen", November 2, 2010, http://www.dawn.com/2010/11/02/us-weighs-options-against-militant-threat-in-yemen.html, (Dec. 7, 2010).

[27] Greg Miller, Greg Jaffe and Karen DeYoung, "U.S. deploying drones in Yemen to hunt for Al-Qaeda, has yet to fire missiles", *Washington Post*, November 7, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/11/06/AR2010110604454_pf.html, (Dec. 9, 2010).

(4) December 17, 2009 and December 24, 2009, two AQAP sites were struck.[28]

These are important successes because they display Yemeni President Ali Salih's resolve to attack al Qaeda bases and operatives, and counters previous rumors that the president owed Osama bin Laden a debt of gratitude for quelling a 1994 separatist movement.[29]

Previous Predator Use in Yemen:

In November 2002 the U.S. ordered a Predator[30] strike on al Qaeda operative, Al Harethi, as his car was driving away from a civilian area.[31] Al Harethi was a key suspect in the U.S.S. Cole bombing of October, 2000.[32] In response the Yemeni government presented a façade of disapproval to assuage the grumbling and complaints of Yemeni citizens, but it is well documented that the Yemeni government increased counter-terrorism cooperation with the U.S. prior to and after November 2002.[33] Previous Yemen counter-terrorism operations to capture Al Harethi on the Yemen-Saudi border cost the Yemen military dearly in December 2001.[34] Criticism of the strike from General Yahya al Mutawakel, Deputy General of the People's Congress Party, concerned not the strike's occurrence, but the acknowledgement that the strike violated a secrecy agreement between Yemen and the United States.[35]

The November 2002 Predator attack is the only known use of Predator UAVs for targeted killing in Yemen. In contrast, the United States has had significant success in targeting al Qaeda and Taliban leaders with UAVs in Pakistan. In September and October 2010, the United States launched 38 UAV attacks in Pakistan. The difference in Predator UAV usage in Pakistan and Yemen is explained as a function of intelligence. Defense experts cite the amount of intelligence on the Taliban and al Qaeda operations in Pakistan is nearing ten years of collection while Yemen collection is just beginning. U.S. officials are signaling that an increase in the number of CIA operatives, U.S. Special Forces teams, and NSA signal intelligence collectors moving into Yemen may rectify the intelligence collection deficiency.[36]

Policy Recommendations:

The above policy indicators of increased military assistance and training, combined with greater intelligence gathering capabilities show that the Obama administration is moving towards increased UAV use in the next 12 to 18 months.[37] This paper recommends that expanded UAV use to launch tactical strikes is not an advisable course of action given the fragile political situation in Yemen. UAVs may bring about tactical success, but will hamper the long-term strategic goals of defeating AQAP for several reasons.

First, UAV targeted killings should not be used in Yemen because counter-terrorism needs to be performed by a police force, not the military. The UAVs should be used for intelligence collection purposes to support the police mission. It should be noted that the Yemeni police were largely responsible for bringing an end to a previous Yemeni terrorist group, Mohammed's Army.[38]

Effective policing in Iraq's Anbar Province in 2006 offers another example of how a state can successfully eradicate al Qaeda's presence. The U.S. assisted Anbar police force gained legitimacy from the local tribal sheikhs that formed the Anbar Salvation Council who were willing to fight al Qaeda in Iraq.[39] This supports the testimony of Mark Cochrane, Former Chief of Training for the Police Service of Northern Ireland, when he asserted that counter-terrorism is a police issue.[40]

To support police efforts Yemeni law makers will need to stop stalling and pass effective counter-terrorism laws. It has been cited that the absence of counter-terrorism legislation enhances Yemen's appeal as a terrorist safe haven and operational base. Yemeni prosecutors often use other vague laws to prosecute terrorists, such as fraudulent document charges or gang membership charges.[41] In addition, the Yemen government will need to invest in secure prisons because they have a history of prison escapes freeing dangerous operatives.[42] For example, in 2006 a group of al Qaeda leaders escaped from a Yemeni prison.[43]

The second reason that the U.S. should avoid expansion of Predator attacks in Yemen is that intervention in the area could create a significant backlash from a population that is "often hostile to the United States."[44] Middle East expert Joost Hiltermann explains that foreign backing of the President Ali Abdallah Salih's regime makes him appear ineffective in controlling the affairs of the country; therefore, the use of UAVs would damage the Yemeni government's legitimacy.[45]

[28] Office of the Coordinator for Counterterrorism, "Country Reports on Terrorism 2009".
[29] William C. Banks, "Legal Sanctuaries and Predator Strikes in the War on Terror", in Michael A. Innes, ed., *Denial of Sanctuary: Understanding Terrorist Safe Havens,* (London: Praeger Security International), p. 117. For more information on the history of Islamist extremism in Yemen in the 1980s and 1990s see: *Al Qaeda in Yemen and Somalia: A Ticking Time Bomb*, p. 11.
[30] For technical information on Predator UAVs see Banks pp. 114-115.
[31] Banks, pp. 116 and 117. This Predator strike was complicated by the death of Kamal Derwish, an American citizen, who was riding in the car with Al Harethi (see p. 120).
[32] Ibid, p. 114.
[33] Banks, pp. 116-17.
[34] Ibid, p. 116. No details were provided on the exact amount of Yemeni military casualties.
[35] Ibid, p. 121.
[36] Miller, Jaffe and DeYoung.
[37] Ibid.
[38] Jones and Libicki, p. 167.
[39] Ibid, pp. 90-94.
[40] Mark Cochrane, "The Importance of Intelligence in Northern Ireland's Conflict – A Practitioner's Perspective", Scowcroft International Affairs Seminar, November 12, 2010.
[41] *Country Reports on Terrorism 2009*.
[42] *Al Qaeda in Yemen and Somalia: A Ticking Time Bomb*, p. 12.
[43] *Yemen on the Brink: Implications for U.S. Policy*, p. 9.
[44] *Al Qaeda in Yemen and Somalia: A Ticking Time Bomb*, p. 8.
[45] Hiltermann, "Disorder on the Border".

Foreign military presence or evidence of their attacks can exacerbate the already hostile attitudes towards the United States and Western allies. In his work, *Dying to Win*, Robert Pape stated:

> Although multiple factors are at work, consideration of the most prominent suicide attacks in 2005 shows that the strategic logic of suicide terrorism—and especially the presence of Western combat forces in Iraq and on the Arabian Peninsula—remains the core factor driving the threat we face.[46]

Robert Pape's position can be seen in the Yemeni context when looking at the effects of the May 2010 cruise missile strikes against AQAP. The attack had deleterious effects on U.S.-Yemen relations because a Yemeni deputy governor was killed who was purportedly was having disarmament negotiations with al Qaeda. Also, locals staged mass protests in Marib Province after they found U.S. markings on cluster munitions. President Salih was forced to respond with troops to quell the tribal protests.[47]

Yemen state officials speak to the drawbacks of potential UAV strikes as being counterproductive. As Mohammed A. Abdulahoum, a senior Yemeni official asked, "Why gain enemies right now? Americans are not rejected in Yemen; the West is respected. Why waste all this for one or two strikes when you don't know who you're striking?"

Conclusion

The U.S. should avoid use of UAVs for targeted killing in Yemen to avoid harming the legitimacy of the Yemen central government and keep counterterrorism in the hands of law enforcement rather than the military. The Yemen state has serious political, social, and economic issues that are compounded by insurgents and terrorists and cannot afford increased instability. To keep the Salih regime as an ally, the U.S. cannot use tools that create local animosity and instability.[48] The U.S. should engage in constructive efforts to build an effective Yemeni police force and counter-terrorism units that can pursue AQAP operatives. These constructive efforts could include UAVs for intelligence gathering purposes, rather than counterproductive missile strikes.

[46] R. A. Pape, Dying to Win: Why Suicide Terrorists Do It, (London: Gibson Square Books, 2006; 1st edn. 2005), pp. v-vi.
[47] Miller, Jaffe and DeYoung.
[48] Banks, p. 123.

Somali Piracy and the Western Response

Brendon Noto

Introduction

September 9, 2010, Captain Alexander Martin and 23 Marines, of the 15th Marine Expeditionary Unit, climbed onboard the Motor Vessel *Magellan Star,* which had been hijacked by Somali pirates the previous day. The boarding was the latest example of the US military's willingness to use force in order to rescue hostage sailors.[1] Western navies have used force to in order to remove Somali pirates from hijacked ships with increased frequency. It is likely that this will result in increased casualties in what was the relatively peaceful practice of Somali piracy.

Piracy became a threat to shipping after the collapse of Somalia's government in 1991, and Somalia's emergence as a, if not *the*, failed state. This threat, which has conjured images of pirates from the Caribbean or the Barbary states, should not be ignored as a threat from the past. Somali pirates have shown the willingness and the ability to attack energy and weapons shipments. The Gulf of Aden is the sea lane used to transport the majority of Europe's oil from the Middle East. If left unchecked piracy could have a negative impact on Western quality of life, and have a destabilizing effect on East Africa.

Piracy is an internationally recognized crime, but Western states have been of two minds about it. America and the European Union (EU), which have shown a willingness to send ships to protect international shipping, lost interest when it was time to prosecute pirates. This duality of purpose was a symptom of how policy makers saw pirates as potential terrorists on one hand, and obsolete criminals on the other. Until Western leaders stop exaggerating the threat of piracy by linking it with terrorism without evidence to support such claims, and ridiculing pirates as an anachronistic threat, they will not develop a coherent policy to address the threat.

Combined Task Forces (CTF) 150 and 151, Operations Atatlanta and Ocean Shield, have shown the Western Navies' ability to divert pirate attacks from the Gulf of Aden to the Indian Ocean. They have also shown the West's inability to stop Somali piracy altogether, something that the Supreme Council of Islamic Courts (SCIC) accomplished, when it consolidated power in southern Somalia. US leaders have spoken about the necessity of a land option in order to end the pirate attacks. If piracy was a threat as dangerous as international terrorism would the US have convinced Ethiopia to invade Somalia in order to evict the fundamentalist Islamic regime?

The US Navy's anti-piracy mission has evolved into its second phase demonstrating policy makers' grudging willingness to see piracy for what it is. The first phase involved the US Navy's use of ships and equipment, which were designed for radically different missions, for anti-piracy operations. The second phase began when the US Navy began transforming its existing resources to the anti-piracy mission. A third phase could further improve US anti-piracy operations if the US Navy designed ships and equipment specifically for anti-piracy operations. If piracy is a result of globalization and failed states, it is only a matter of time before the third phase becomes a reality because piracy will spread to other failed states in littoral regions.

Piracy will persist until there is a stable government that pacifies Somalia. There are steps that can and should be taken in order to discourage piracy and promote stability in Somalia until that happens. Adapting and designing resources for the anti-piracy mission is just one of those steps. Others include prosecuting pirates, arming merchant ships that transport critical supplies, and supporting the African Union's (AU) peacekeeping efforts in Somalia. It is up to the Somali people to eliminate the practice of piracy in the Horn of Africa (HOA), but the West can, and should, take all necessary measures to prevent it, and to create an atmosphere that encourages the formation a stable government in Somalia.

I: Somali History

When World War II ended, Great Britain ruled over a unified Somalia. In the 1950's, Somalia was divided between British and Italian UN Trusteeships.[2] In July 1960, the two territories were granted independence.[3] Somalia's President Abdi Rashid Ali Shermarke was assassinated in 1969, and Major General Mohamed Siad Barre took over the reins of the Somali government.[4] Barre ruled Somalia during the 1970s and 1980s, but stability under Barre would not last.[5] Though the Barre government did not fall until January 1991, "ample evidence suggests that by the mid-1980s Somalia was already a failed state."[6] Once Barre was deposed, Somalia fell into civil war and broke apart into regions

[1] Alexander Martin, "Evolution of a Ship Takedown," *Proceedings,* 136 (November 2010), 38-41, and Alexander Martin, "The Magellan Star: Pirate Takedown, Force Recon Style," *US Naval Institute,* September 2010, *available at* http://blog.usni.org/2010/09/10/the-magellan-star.

[2] "Somalia - Trusteeship and Protectorate: The Road to Independence," *Country Studies*, *available at* http://countrystudies.us/somalia/14.htm (accessed October 14, 2010).

[3] Kenneth John Menkhaus, "Governance without Government in Somalia Spoilers, State Building and Politics of Coping," *International Security,* 31, no. 3 (2006): 74-106.

[4] Dr. Rannee Khooshie Lal Panjabi, "The Pirates of Somalia: Opportunistic Predators or Environmental Prey?" *William & Mary Environmental Law & Policy Review,* 34, no. 1 (2010): 396.

[5] Kimberly Zisk Marten, "Warlordism in Comparative Perspective," *International Security,* 31, no. 3 (2006): 52.

[6] Menkhaus, 80.

ruled by warlords, the most powerful being General Mohammed Farah Aideed.

In 1992, warlords agreed to a ceasefire, United Nations (UN) intervention arrived in the form of UNOSOM I, and "at this point, President George H.W. Bush made the fateful decision to lead a large-scale international intervention to halt the mass starvation."[7] Later under President Bill Clinton, the US would lead UN Operation Restore Hope and UNOSOM II, a more ambitious policy with less clearly defined goals. As a result of the Mogadishu incident on October 3-4, 1993, when 18 American soldiers died, the US decided to abandon its effort to restore stability to Somalia.[8]

After the failure of Operation Restore Hope, Somalia has not had a unified government. Despite resistance from the international governing bodies to recognize breakaway governments, Somalia has split into three separate regions because "Somaliland and Puntland, have separated the former declaring independence in 1991 and the latter declaring autonomy in 1998."[9]

Somaliland and Puntland

Somaliland has enjoyed a stable government since 1996, despite a lack of international recognition. Kenneth Menkhaus reported, "Somaliland has also built up a modest but functional state structure."[10] Somaliland has been relatively peaceful compared to the rest of Somalia because its population has strong clan ties and its clans have promoted peace.[11] Other factors include support of business leaders, President Egal's leadership, and the population's "commitment… to peace and rule of law," which has helped unify the society.[12]

The international community refuses to support Somaliland because "the rest of Somalia does not want it,"[13] and there are fears that it could set a precedent that would spark future breakaway states in other African countries.[14] By granting support to the Somali Transitional Federal Government (TFG) as opposed to the government of Somaliland, the international community shows a lack of understanding of Somalia's political situation and a refusal to engage in policies that help the Somali people.

Puntland was the second unrecognized breakaway region of Somalia, and most pirate activity is based out of this region, which calls into question the ability or the will of the Puntland government to police its own territory.[15] Puntland's port city Eyl is a notorious pirate haven.[16] Nevertheless, the Puntland government claims to support the Transitional Constitution and "is striving for the unity of the Somali people and the creation of a Somali government."[17]

Somalia

The southern half of Somalia has lacked an operational government since General Barre was overthrown in 1991 and serves as "the longest-running instance of complete state collapse in postcolonial history."[18] In 2008, 2009, and 2010, *Foreign Policy* ranked Somalia the most failed state in the world,[19] and it has been in the top ten since the Failed State Index was created in 2005.[20] Somalia has seen the rise of two major radical Islamic militias and has been a haven for warlords and civil war. UN food aid is a common target of theft by warlords, which, when coupled with a major drought, has contributed to the displacement of over a million people, causing half a million refugees to flee Somalia.[21] The international community supported the creation of the TFG in 2004, "the latest of more than a dozen attempts to re-create a functioning state… yet remained unable even to establish a base in Mogadishu."[22] The TFG governed Somalia from Kenya in 2006, and President, Abdullahi Yusuf Ahmed, did not appear in Mogadishu until 2007 due to the TFG's inability to control large areas of the country.[23]

By 2006, the SCIC, also called the Union of Islamic Courts (UIC), had achieved dominance over most of southern and central Somalia and brought order to Mogadishu.[24] The SCIC banned the charcoal and drug trades,[25] effectively stamped out piracy in areas it controlled,[26] and took active steps to combat piracy.[27] Anthony Davis said:

---

[7] R.D. Hooker, JR, "Hard Day's Night: A Retrospective on the American Intervention in Somalia," *Joint Force Quarterly,* 54, no. 3 (2009): 129.

[8] Ibid., 133, and Michael Miklaucic, and Robert B. Oakley, "Essay 18 Beyond the Cold War: Pakistan and Somalia," In *Commanding Heights: Strategic Lessons From Complex Operations,* Washington DC: *The Center for Complex Operations and the Center for Technology and National Security Policy*, 2009. 145-47.

[9] Panjabi, 406.

[10] Menkhaus, 91.

[11] Marten, 53.

[12] Menkhaus, 93.

[13] "Somaliland A Nomad's Life is Hard," *The Economist*, August 55, 1999, *available at* http://www.economist.com/node/230314/print.

[14] Menkhaus, 92.

[15] Mohammed Adow, "The pirate kings of Puntland," *AJE - Al Jazeera English*, 16 Oct. 2010, *available at* http://english.aljazeera.net/news/africa/2009/06/2009614125245860630.html.

[16] Mary Harper, "Life in Somalia's pirate town," *BBC News,* 18 Sept. 2008, 16 Oct. 2010, *available at* http://news.bbc.co.uk/2/hi/7623329.stm.

[17] "Puntland State Profile," *Puntland,* 15 Oct. 2010, *available at* www.puntland-gov.net/profile.asp.

[18] Menkhaus, 74.

[19] "The 2010 Failed States Index," *Foreign Policy,* 16 Oct. 2010, *available at* http://www.foreignpolicy.com/failedstates.

[20] "The Failed States Index," *Foreign Policy,* Jul/Aug.149 (2005): 56-65.

[21] Panjabi, 392.

[22] Marten, 53.

[23] Panjabi, 407.

[24] Menkhaus, 100.

[25] Ibid,, 90.

[26] Panjabi , 412.

[27] Frederic P. Miller, Agnes F. Vandome, and John McBrewster, *Piracy in Somalia: Piracy in Somalia, International Maritime Bureau, List of ships attacked by Somali pirates, Operation Enduring Freedom - Horn of Africa, Operation Atatlanta, Combined Task Force 150, Basel Convention* (Hagerstown: Alphascript, 2009), 1.

> The UIC announced that they would punish those engaged in piracy... For a time the incidents ceased, until they struck the United Arab Emirates cargo ship, *MV Veesham I*… The UIC in response… recaptured the vessel and rescued the crew after a gun battle with the pirates.[28]

The lull in piracy did not last because international politics portrayed the SCIC as Islamic fundamentalists. The potential threat of a jihadist government in Somalia outweighed the SCIC's anti-piracy policy to Western policy makers.

Due to the perceived threat from the SCIC, and US pressure to destroy a potential Islamic terrorist sponsor, Ethiopia – a regional United States ally – invaded Somalia in late 2006 and brought down the SCIC.[29] At the Djibouti Peace Agreement of 2008, Ethiopia, agreed to withdraw its troops.[30] In the power vacuum created by the Ethiopian invasion the Shabab Militia emerged as the dominant player in southern Somalia.[31] Andre Le Sage said its success was "less an indicator of its own strength, and more a function of the weakness of... the TFG."[32] The Shabab Militia has been linked to al-Qaeda, including running terrorist training camps, and stopped UN food aid shipments. *The Economist* reported that "*Shabab*, is even more radical than the Islamic Courts movement which the Americans and Ethiopians originally took on. It is suspected of being linked by money to the pirates… and by ideology to al-Qaeda."[33] Thus international support for the TFG has led to the eviction of the SCIC, who combated piracy and crime, and has caused the rise of the Shabab Militia a group tied to both al-Qaeda and pirates.

II: Modern Piracy

Modern piracy originates primarily from failed states. In order to eliminate confusion that may arise from the use of terms, two terms will be defined: failed state, and piracy. A failed state, according to the Crisis State Research Center, is a state that is in

> A condition of "state collapse" – e.g. a state that can no longer perform its basic security, and development functions and that has no effective control over its territory and borders. A failed state is one that can no longer reproduce the conditions for its own existence.[34]

Thus a failed state has no functional government, military, and lacks control over its borders. This applies to southern and central Somalia since 1991. Piracy as defined by the UN in the "Convention of the Law of the Sea"

> *Article 101 Definition of Piracy*
> *Piracy consists of any of the following acts:*
>
> *(a)* any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed:
> (i) on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft;
> (ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;
> (b) any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft;
> (c) any act of inciting or of intentionally facilitating an act described in subparagraph (a) or (b).[35]

In summary, piracy is a violent attack committed on the "high seas" by private individuals. Somalia is a failed state since 1991, and Somalis who commit violent acts, such as hijacking ships in the Gulf of Aden or the Indian Ocean are pirates.

Types of Piracy

The International Maritime Bureau (IMB) outlined three types of piracy: "Low-Level Armed Robbery… Medium-Level Armed Assault and Robbery (MLAAR)… and Major Criminal Hijack." Somali piracy most resembles MLAAR, which is described as "attacks from well organized gangs comprising 10 to 30 heavily armed men… pirates, especially off Somalia… take crew members hostage."[36] Somali pirates rarely kill prisoners; most violent deaths resulted from shootouts with naval personnel who attempted to free the prisoners.[37]

There are three areas where "the attack occurs: Piracy At Pier… Piracy At Anchorage… Piracy Against Ships Underway," and though there have been instances of food aid being hijacked at pier, the vast majority of

[28] Anthony M. Davis, *Terrorism and the Maritime Transportation System Are We on a Collision Course?* (Livermore: Wingspan 2008) 119-20.
[29] Napoleon A. Bamfo, "Ethiopia's Invasion of Somalia in 2006: Motives and Lessons Learned," *African Journal of Political Science and International Relations,* 4:2 (2010): 59-61.
[30] "Modalities for Implementation of Cessation of Armed Confrontation," *United Nations Political Office for Somalia,* 26 Oct. 2008, 18 Oct. 2010, *available at* unpos.unmissions.org/Portals/UNPOS/Repository%20UNPOS/081026%20-%20Modalities%20for%20Implementation%20of%20Cessation%20of%20Armed%20Confrontation.pdf.
[31] Andre Le Sage, "Somalia's Endless Transition: Breaking the Deadlock," *Strategic Forum,* 257 (2010): 1-2. *CSR Strategic Forum*. Web. 18 Oct. 2010.
[32] Le Sage, 4.
[33] "Somaliland Anarchy in Somalia: The Lawless Horn," *The Economist*, November 20, 2008, *available at* http://www.economist.com/node/12637009/print.
[34] "Crisis, Fragile and Failed States Definitions used by the CSRC," *Crisis State Research Center*, *available at* www.crisisstates.com/download/drc/FailedState.pdf.
[35] "Preamble to the United Nations Convention on the Law of the Sea," *United Nations*, *available at* http://www.un.org/Depts/los/convention_agreements/texts/unclos/part7.htm.
[36] Michael Stehr, "Modern Piracy: Growing Threat to Shipping, Counter Threat Technology and Tactics," *Naval Forces,* 26, no. 5 (2005): 20.
[37] David Axe, "10 Things You Didn't Know About Somali Pirates," *Wall Street Journal*, April 27, 2009, *available at* http://online.wsj.com/article/sb124060718735454125.html?KEYWORDS=somali+piracy.

Somali acts of piracy have been against ships underway and

> Piracy against ships underway offers a lot of opportunities but requires also some nautical abilities and suitable vessels. There are three variants… short-term seizure… long-term seizure… permanent seizure… the pirates are usually heavily armed with automatic weapons, grenade launchers and other military equipment.[38]

Somali piracy most resembles "long-term seizure where pirates are stearing the ship to a secret place," and from there the pirates demand a ransom for the ship, cargo and crew.[39]

Piracy and Terrorism

The US Navy leadership exaggerates the threat posed by piracy by linking pirates to terrorists and downplays the threat by comparing modern pirates with their historical counterparts. The threat to international shipping is relatively small, with the exception of energy shipments, but raises the cost of shipping. However, piracy has only been linked to terrorism by superficial associations.

US Navy Chief of Naval Operations (CNO) and Secretary's of the Navy (SECNAV) call pirates terrorists or try to link the two. Statements by Navy leaders show that linking piracy and terrorism was US Navy policy. In 2003 CNO Vern Clark said "pirates [are] conducting premeditated, politically motivated violence against innocent seafarers. That is using terror, that's terrorism."[40] In 2004 SECNAV England said "terrorists have already shown an ability to exploit the seas with attacks such as USS Cole and links to piracy and smuggling."[41] In 2005 CNO Mullen warned that piracy could shut down important sea lanes:

> Piracy… It is a global threat to security because of its deepening ties to international criminal networks, smuggling of hazardous cargoes, and disruption of vital commerce. Imagine a major seaport or international strait that handles the flow of hundreds of ships and thousands of containers each day – imagine that critical "node" of the world's economy crippled or disrupted for days or weeks or months.[42]

Oil shipments are particularly vulnerable to pirate attacks due to their low freeboard (the distance between water and deck of a ship). Yet, it is an exaggeration to imply that Somali pirates would be able to blockade a major straight, such as the Gulf of Aden, for days on end. The US fifth and sixth fleets maintain a constant presence in the vicinity of the choke points that connect the Mediterranean Sea and the Persian Gulf.

US Navy leadership had a policy of equating piracy with terrorism, linking pirate networks with terrorist networks, and making piracy appear as dangerous to international and US national security as terrorism, and implied piracy was a critical threat to maritime security. Furthermore, the claim could be made that Somali pirates were eco-terrorists, but eco-terrorism is not as dangerous to international order as jihadist terrorists such as al-Qaeda. The threat of Somali eco-terrorism, if Somali eco-terrorists exist, does not extend beyond the confines of Somali territorial waters. Yet claims that Somali pirates were dangerous to world order have been made along with comments that compare the Somali pirates to the Barbary corsairs. This shows a duality of US naval policy. Pirates were both dangerous and comical. In 2006, CNO Mullen both compared the Somali pirates with their eighteenth century counterparts and exaggerated the threat when he said:

> Globalization… terrorists, proliferators of W-M-D and other weapons, organized criminals, smugglers, drug traffickers and pirates. Yes, pirates. Only today they sail the seas with satellite phones and laser-guided weapons instead of cutlasses and muskets.[43]

Most recently CNO Roughead stated that

> Consider the age old naval task of convoying... this was something we did in our navy to counter the Barbary pirates in the 19th century... if you think the value of convoying or protecting trade has diminished: consider the Gulf of Aden… the threat of pirates against commercial shipping in the Gulf of Aden was enough of a concern to bring together an international Fleet of ships.[44]

The US Navy has a proud heritage and enjoys relating current events to past victories; however this practice can confuse the issue. The Barbary pirates have little in common with their Somali counterparts. Rather than connecting piracy with terrorism, exaggerating the threat of piracy, or making pirates appear like something from the past, Navy leaders should address the true threat that piracy poses to the international community and regions directly affected.

---

[38] Stehr, 20-21.

[39] Ibid.. 21.

[40] Vern Clark, "Edited Remarks," Speech, *International Seapower Symposium*, Naval War College, Newport, R.I. October 27, 2003, *available at* http://www.navy.mil/navydata/people/cno/speeches/clark031027.txt.

[41] Gordon R. England, "Remarks By," Speech, *The Naval Institute Warfighter's Symposium*, Virginia Beach, VA, September 29, 2004, *available at* http://www.navy.mil/navydata/people/secnav/England/speeches/england040929.txt.

[42] Mike Mullen, "Remarks as Delivered for the 17th International Seapower Symposium," Speech, *National Defense University*, Washington, DC, August 16, 2005, *available at* http://www.navy.mil/navydata/people/cno/mullen/speeches/mullen050921.txt.

[43] Mike Mullen, "Remarks as Delivered," Speech, *Current Strategy Forum*, *Naval War College*, Newport, RI. June 14, 2006, *available at www.navy.mil/navydata/people/cno/mullen/cno_csf140606.pdf.*

[44] Gary Roughead, "Delivers Remarks at the Conference of Defense Associations," Speech, *Conference of Defense Associations*, Ottawa, Canada. March 3, 2010, *available at* http://www.navy.mil/navydata/people/cno/Roughead/Speech/100303%20Remarks%20as%20delivered%20at%20the%20Conference%20of%20Defence%20Associations%20FINAL.doc.

Experts have disagreed with the pirate-terrorist link for example Martin Murphy stated that "when it comes to piracy itself, there is no worthwhile evidence, despite the speculation, of any cooperation between pirates and insurgent/terrorists,"[45] and in *Small Boats, Weak States, Dirty Money* he wrote:

> Since the events of 9/11, a strain in security discourse has yoked piracy and maritime terrorism together; has viewed them as complementary to the point where some commentators has suggest that a "piracy-terrorism' nexus exists or might exist in the future. The impetus behind this can again be traced to the false analogy between aircraft and ships which led to the suggestion that pirates could help terrorists learn how to steal and control ships for attack purposes. 'Nexus' is an evocative word that needs to be used with care because, in this context, it can gloss over the motivational and operational reasons that generally keep criminals and terrorists apart and imply an instrumentality that does not exist.[46]

Thus if the Somali pirates are not connected to terrorists, the final question regarding this subject is, are Somali pirates eco-terrorists?

Some Somali pirates claim that they are protecting their waters from over fishing and toxic waste dumping, and as early as 1995 Somali political leaders complained about the illegal practices to the UN and EU.[47] No exact figures exist, but it was estimated that Somali fishermen lose roughly $100 to $300 million a year due to foreign ships illegally fishing in Somali waters.[48] After the 2004 tsunami, the UN acknowledged that barrels which contained nuclear waste had washed up on Somali shores, and believed that the Somali people were being poisoned by the toxic waste that had been dumped in their waters.[49] In response to the illegal activity during the 1990s, Somali fishermen joined forces and began charging foreign fishermen a toll to fish in Somali waters.[50] Though the Somali pirate-fishermen may have had a noble beginning, the situation changed. As the US State Department commented, "pirates... conduct violent attacks up to 1,000 miles and more from Somalia's shores on private yachts, passenger cruise liners, and commercial vessels such as tankers and container ships that are clearly not involved in fishing."[51] Somali pirates may have begun their operations targeting foreign fishermen, but they descended into profiteering and criminality.

Somali pirates fit the definition of piracy; they are not state-sponsored and they commit violence on the high seas. They are not terrorists, and there are no verified links that connect Somali pirates with terrorists. Somali pirates are criminals and the threat they pose to the international community and East Africa should not be exaggerated, nor blown off as a comical anachronistic threat indicative of the distant past.

III: Somali Piracy

Money is the motivating force behind Somali piracy. Somalia has no functional economy, and ransom payments from hijacked ships inject millions of dollars into the region. It was estimated that in 2008, ransoms injected $35 million into Puntland's economy. Piracy has also become a prestigious career due to the relative wealth of pirates compared to average Somalis.[52] The average pirate is believed to make more than $20,000 each year,[53] compared to the average per capita GDP of Somali of around $600 a year; the average pirate is rich.[54] Perhaps as much as 20% of the ransom money is reinvested in the Somali economy,[55] but David Axe said that "bosses can pull in $2 million a year... many pirates are heading for greener pastures, and real money is flowing out of the country with them."[56] Thus, piracy for Somalia is a mixed blessing. It injects cash into the economy, but this causes detriments including inflation and the fear of piracy, which has forced the UN to use more expensive overland food aid shipments, and most of the ransom money leaves Somalia.[57]

Pirate Tactics and Methodology

The pirates operate off of the eastern coast of Somali, and, according to the *BBC*, there are three types. *BBC*'s Mohamed Mohamed, said that the first type of pirate is the "Ex-fishermen," the second is the "Ex-militiamen," and the third are "technical experts who operate equipment."[58] Pirates are said to be between 20-35 years old and originate from the Puntland region.[59] The pirate groups operate out of coastal cities,

---

[45] Martin N. Murphy, "Suppression of Piracy and Maritime Terrorism. A Suitable Role for the Navy?" *Naval War College Review*, 60.3 (2007): 31.
[46] Martin N. Murphy, *Small Boats, Weak States, Dirty Money: Piracy and Maritime Terrorism in the Modern World* (New York: Columbia 2009) 380.
[47] Panjabi , 423.
[48] Lesley Anne Warner, "Pieces of Eight: An Appraisal of U.S. Counterpiracy Options In the Horn of Africa," *Naval War College Review*, 63.2 (2010) 62 and Lauren Ploch; Christopher M. Blanchard; Ronald O'Rourke; R. Chuck Mason; Rawle O. King, "Piracy Off the Horn of Africa," Congressional Research Service, April 19, 2010, 10.
[49] Panjabi , 430.
[50] Ibid., 434 and Axe, "10 Things You Didn't Know About Somali Pirates."
[51] "Setting the Record Straight: No Justification for Piracy Off the Coast of Somalia," *U.S. Department of State*, December 17, 2009, http://www.state.gov/r/pa/prs/ps/2009/dec/133784.htm.
[52] Panjabi, 447-48.
[53] "Somalia's Pirates: A Long War of the Waters," *The Economist*, January 7, 2010, *available at* http://www.economist.com/node/15214052/print.
[54] "World Factbook," *Central Intelligence Agency*, *available at* https://www.cia.gov/library/publications/the-world-factbook/geos/so.html.
[55] Panjabi , 448.
[56] Axe, "10 Things You Didn't Know About Somali Pirates."
[57] Anthony Mitchell, "Pirates hijack UN food aid ship," *The Guardian*, *available at* http://www.guardian.co.uk/world/2007/feb/26/international.mainsection/print.
[58] Robyn Hunter, "Somali pirates living the high life," *BBC News, available at* http://news.bbc.co.uk/2/hi/7650415.stm.
[59] Miller, 4.

the most notorious of which is Eyl,[60] and there are said to be at least four pirate groups.

> Four main pirate groups are operating along the Somali coast. The National Volunteer Coast Guard… The Marka group… The third significant pirate group is composed of traditional Somali fishermen operating around Puntland and referred to as the Puntland Group. The Somali Marines are the most powerful and sophisticated of the pirate groups.[61]

Martin Murphy said:

> Much attention was devoted to curbing the activities of the 'Somali Marines', which during its first active period, from 2005-2006, was the most effective pirate gang operating off Somalia. It stood out because it was willing to venture far out to sea… their competence in general, should not be exaggerated… early in 2007 there was a report that pirates were re-assembling at Xaradheere, the 'Somali Marines' former base… the suspicion is that it is the reinvigorated 'Somali marines' that have been responsible for most, if not all, of the large scale piracy that has taken place off Somalia in the period between the ICU's collapse in 2006 and early 2008.[62]

Thus, the most common Somali pirates are in their twenties and thirties, and former fishermen.

Pirate towns are located in Puntland and the ungoverned region of Southern Somalia. According to the National Security Council (NSC), "Somali pirates operate from well-equipped and well-armed bases ashore along the Indian Ocean coast of Central Somalia and Puntland, from the port towns of Caluula, Eyl, Hobyo, and Haradheere [Xaradheere]."[63] Caluula and Eyl are located within Puntland and Hobyo and Haradheere are in central Somalia. Eyl has benefitted the most from piracy revenues which has funded new building construction that caters to the needs of the pirates.[64] The pirates also operate out of Yemen, which they use a resupply point, and they utilize the ports of Al Mukalla and Ash Shihr in Yemen, Mogadishu in Somalia, and Bosaso in Puntland as bases for their 'mother ships.'[65] Thus it is not only the lack of effective government in Somalia that encouraged piracy, but also a lack of Yemeni deterrence.

Mother ships are formerly pirated fishing dhows, sailing vessels that are used to launch motor boats.[66] This extends the range that the pirates can operate and is a major factor why piracy attacks have occurred as far away from Somalia as the island nation of the Seychelles. Pirates attack other ships in speed boats that are "equipped with satellite phones and GPS equipment,"[67] and "typically armed with military assault rifles and rocket-propelled grenades."[68] In order to board the targeted ships the pirates can use grappling hooks or an "aluminum ladder."[69] Jeevan Vasagar said that "attacks typically begin with pirates firing distress flares as a means of luring passing ships… men armed with automatic weapons and rocket-propelled grenade launchers rush towards the ship in speedboats, aiming to cut off escape by approaching from different directions."[70] In order to force the ships to submit the pirates will "fire upon their targets with small arms, automatic weapons, and rocket-propelled grenades."[71] Anthony Davis, explained why cargo ships will stop and allow the pirates onboard

> Even though the cargo ship is much larger than the pirate boat, just a few sailors operated them. If attacked by an RPG, the ship becomes vulnerable to fire… When combating a fire, the ship must stop or else the prevailing wind caused by the forward motion of the vessel feeds the fire… A minimal crew with no security protection stands little chance of successfully fighting a fire and out maneuvering a smaller, faster boat armed with weapons.[72]

Thus the crew of the cargo ship has a choice between risking a fire at sea or capture by pirates.

Once the pirates are onboard they take the vessel, crew, and cargo hostage, and pilot the vessel into Somali waters. From there they contact the vessel's owner and demand a ransom. According to the IMB

> Pirates say ransom money is paid in large denomination US dollar bills. It is delivered to them in burlap sacks which are either dropped from helicopters or cased in waterproof suitcases loaded onto tiny skiffs. Ransom money has also been delivered to pirates via parachute.[73]

The ship's owners usually pay the ransom with money received from "ocean marine insurance," that covers events such as piracy, and in return the pirates do not harm the ship or the crew.[74] The negotiations usually involve middle men, Somalis that live in Europe

---

[60] Panjabi, 447.
[61] "Pirates," *GlobalSecurity.org, available at* http://www.globalsecurity.org/military/world/para/pirates.htm
[62] Murphy, *Small Boats, Weak States, Dirty Money*, 104-105.
[63] *Countering Piracy Off the Horn of Africa: Partnership and Action Plan*, *National Security Council*, 2008, *MERLN*, *available at* http://www.marad.dot.gov/documents/Countering_Piracy_Off_The_Horn_of_Africa_-_Partnership_Action_Plan.pdf, and Dr. Muhammad S. Megalommatis, "The MV FAINA Piracy Crisis Chronicle," *California Chronicle*. December 07, 2008. <http://www.californiachronicle.com/articles/view/84087.
[64] Panjabi, 447.
[65] Ploch, 11.
[66] *Countering Piracy Off the Horn of Africa: Partnership and Action Plan*, 5.
[67] "Pirates hijack UN food aid ship," *Guardian,* http://www.guardian.co.uk/world/2007/feb/26/international.mainsection/print.
[68] "Setting the Record Straight: No Justification for Piracy off the Coast of Somalia."
[69] Axe, "10 Things You Didn't Know About Somali Pirates."
[70] Jeevan Vasagar, "Pirates hijack tsunami aid ship," *The Guardian*, *available at* http://www.guardian.co.uk/society/2005/jul/01/internationalaiddanddevelopment.internationalnews.
[71] *Countering Piracy Off the Horn of Africa: Partnership and Action Plan*, 5.
[72] Davis, 121.
[73] Miller. 5.
[74] Rawle O. King, "Ocean Piracy and Its Impact on Insurance," *Congressional Research Service*, February 6, 2009, 1.

or the Middle East, and if the money is transferred overseas, it is funneled into Somalia.[75]

The crews of the hijacked ships are usually well taken care of because it is good business to keep the prisoners alive. The hostages are worth ransom money and if the hostages are returned alive foreign navies have little incentive to risk rescue missions.[76] Somali pirates are able to ask for, and receive, ransom money because they have the unique ability to bring the pirated vessel into the safety of Somali waters. Pirates from other countries do not have the ability to keep a ship for months on end as they negotiate the ransom.[77] If pirate safe-havens were removed Somali pirates may resort to traditional hit-and-run tactics that are practiced by pirates in other parts of the world. The average ransom has been estimated to be between $1 and $2 million and rising.[78] As the ransom amounts increases, so have the number of pirate attacks.

Pirate Attacks

Somali piracy has risen since the late 1990s. International efforts to prevent it have had little effect on the number of attacks. The one period that saw a decrease in attacks was when the SCIC controlled most of southern Somalia. International efforts have had an impact on the location where the attacks occur, but almost none on preventing attacks. Pirates have adapted to new tactical environments. Pirate activity is also affected by the time of the year, less pirate activity takes place during the two monsoon seasons.

The IMB Piracy Reporting Center has tracked the number of pirate attacks off the coast of Somalia, in the Indian Ocean, Red Sea, Gulf of Aden and Gulf of Oman, the areas where Somali pirates were the most active. The IMB stated that off the coast of Somali 35 attacks occurred in 2005, 10 in 2006, 31 in 2007, 19 in 2008, and 80 in 2009. In the Indian Ocean one attack occurred in 2005, and one in 2009. The Red Sea only had pirate attacks in 2009, when there were 15. The Gulf of Aden had 10 attacks in 2005, 10 in 2006, 13 in 2007, 92 in 2008, and 116 in 2009. Eritrea, Kenya, Madagascar, Oman, Tanzania, and the Seychelles are also victims of Somali piracy and between them saw 8 attacks in 2005, 9 in 2006, 20 in 2007, 17 in 2008, and 10 in 2009. In all the areas of Somali pirate activity, there were 54 attacks in 2005, 29 in 2006, 61 in 2007, 128 in 2008, and 222 in 2009.[79] Thus the number of attacks have doubled two years in a row from 2006, to 2008, and nearly doubled again in 2009. These trends are supported by IMO statistics.

The IMO also reported an increase in pirate attacks in 2009, compared to 2008. In 2008 the IMO reported 160 attacks committed and attempted,[80] 415 in 2009,[81] and 41 in the first quarter of 2010.[82] The difference may come from a deviation in the definition of piracy and that the IMB relies on voluntary reports of pirate attacks. Both records show an increase in piracy between 2008 and 2009. The low number of attacks reported by the IMO in the first quarter of 2010 was most likely due to the monsoon seasons which run from "May and September and from December to March."[83] The Office of Naval Intelligence (ONI), lists weather as "the primary factor determining when pirates will operate."[84] In April, when the monsoon season ended, it is likely that piracy escalated. The IMB's report for the first three quarters of 2010 confirmed that. There have already been 44 attacks in the Gulf of Aden, 56 in Somali waters and 24 in the Red Sea.[85] Compare those numbers with 2008, which had 19 in the Gulf of Aden, 92 in Somali waters, and 0 attacks in the Red Sea. Thus 2010, has already had more pirate attacks than 2008, and the May – September monsoon season has ended which should allow for a sharp increase in attacks for the remainder of the year. A change in the pattern of attacks from January – September of 2009, and 2010, was that attacks in the Gulf of Aden have reduced, and attacks in Somali waters and the Red Sea have increased.

The increase in piracy is a sign that increased international efforts have had little impact in reducing Somali piracy. The international community, led by the United States, has increased anti-piracy operations off of the HOA. In 2009, the height of Somali piracy, was when "The Combined Maritime Forces established CTF 151 Jan. 8 specifically for counter-piracy operations."[86] CTF-151 broke off from CTF-150, which was created "with

[75] Julian Borger, "Piracy and ransom payments: Risky business - safe transactions," *The Guardian,* November 11, 2008, *available at* http://www.guardian.co.uk/world/2008/nov/19/piracy-somalia1.

[76] Axe, "Ten Things You Didn't Know About Somali Pirates."

[77] Ploch, 12.

[78] "Somalia's Pirates: A Long War of the Waters."

[79] "Piracy and Armed Robbery Against Ships: Annual Report 2009," *International Maritime Bureau*, *available at* www.mfa.gr/softlib/%CE%95%CF%84%CE%AE%CF%83%CE%B9%CE%B1%20%CE%B1%CE%BD%CE%B1%CF%86%CE%BF%CF%81%CE%AC%20%CE%B3%CE%B9%CE%B1%20%CF%84%CE%.

[80] "Reports On Acts of Piracy and Armed Robbery Against Ships: Annual Report 2008," *International Maritime Organization*, *available at* www.imo.org/OurWork/Security/PiracyArmedRobbery/Monthly%20and%20annual%20piarcy%20and%20armed%20robbery%20report/133-Annual2008.pdf.

[81] "Reports On Acts of Piracy and Armed Robbery Against Ships: Annual Report 2009," *International Maritime Organization*, *available at* http://www.imo.org/OurWork/Security/PiracyArmedRobbery/Monthly%20and%20annual%20piarcy%20and%20armed%20robbery%20report/152-Annual2009.pdf.

[82] "Reports On Acts of Piracy and Armed Robbery Against Ships: First Quarterly Report," *International Maritime Organization*, *available at* http://www.imo.org/OurWork/Security/PiracyArmedRobbery/Monthly%20and%20annual%20piarcy%20and%20armed%20robbery%20report/153-1Q2010.pdf.

[83] Warner, 73.

[84] "Horn of Africa: Threat Factors for Commercial Shipping and Forecast of Pirate Activity Through 2009," *US Department of Transportation Maritime Administration*, *available at* www.marad.dot.gov/documents/Factors_Affecting_Pirate_Success_HOA.pdf .

[85] "Piracy and Armed Robbery Against Ships: Report for the Period 1 January – 30 September 2010," *International Maritime Bureau*.

[86] "New Counter-Piracy Task Force Established," *The U.S. Navy*, January 9, 2009, *available at* http://www.navy.mil/search/display.asp?story_id=.

the intent to preclude the use of sea by terrorists to move weapons and personnel"; it is a coalition task force that has been dedicated to preventing piracy, over the time period that the Horn of Africa saw the greatest increase in piracy.[87] President George W. Bush also created the United States African Command, which "aims to address the roots of instability by promoting civil and defense sector reforms, military professionalism, and capacity-building programs which allow Africans to help themselves."[88] Yet the only group that has decreased Somali piracy was the SCIC. Most experts look for a solution inside Somalia to end piracy because operations at sea have not solved the problem. The US Secretary of Defense Robert Gates agreed when he said that "there is no purely military solution to it," and that "there's really no way in my view to control it unless you get something on land that begins to change the equation for these kids."[89]

Specific Attacks

Three pirate attacks that have received the most international attention: the MV *Sirius Star*, the MV *Faina*, and the MV *Maersk Alabama.* Each attack became notorious for different reasons, but what they had in common was a blatant disregard for the established international power structure. Pirates challenged the power of Saudi Arabia, the world's leading oil supplier,[90] Russia the former Soviet super power, and the United States, the remaining super power. The *Sirius Star,* which transported 2 million barrels of crude oil, was attacked on November 15, 2008; the *Faina,* transporting 33 T-72 Main Battle Tanks as well as anti-aircraft guns and small arms,[91] was attacked September 25, 2008;[92] and the *Maersk Alabama,* transporting food aid,[93] was attacked on April 8, 2009.[94]

By seizing the *Sirius Star* the pirates showed that they were not a Pan-Islamic movement because they would not respect the sovereignty of a Muslim power. The attack on a Muslim flagged ship showed an independence of action that reinforces the categorization that pirates are criminals and not jihadist terrorists. The seizure of the *Faina* was the attack that showed the world that pirates and Somali pirates in particular, are dangerous. Had the pirates unloaded the tanks into Somali, *The Economist* said it would be "enough to tip the balance in a small local war."[95] The *Faina* had three Russian crew members and the attack provoked Russia into sending a frigate to patrol the Horn of Africa.[96] In the ultranationalist Putin era Russia, it is likely that the *Faina* attack was an insult to Russian national pride.[97] The *Faina* incident showed that Somali pirates could become more than an economic nuisance. Finally the *Maersk Alabama* was the first successful attack on an American flagged ship by Somali pirates. This was a direct challenge to US supremacy. Captain Richard Phillips was saved when Navy SEAL "snipers… killed three pirates holding him at gunpoint."[98] Thus Somali pirates have defied regional powers that they are linked to by religion, European powers, and America the global super power. In the case of the *Sirius Star* and the *Faina* the pirates received a ransom and returned the ship, however when the pirates challenged the power of the US that they were killed. Most importantly, these cases brought attention to the problem and showed that if left to its own devices the problem could escalate.

Global Shipping

The Gulf of Aden is a choke point that makes ships easier targets than they are in open seas. The narrow Gulf is a mixed blessing for pirates because it also makes it easier for warships to patrol due to the concentrated number of ships. A warship can protect a larger number of ships than it could in the Indian Ocean. It is not only the number of ships that makes the Gulf of Aden an important shipping lane, but also the cargo.

More than 20,000 ships travel through the Gulf of Aden every year.[99] Between 11-33% of the world's crude oil passes through the Gulf[100] and "over 80% of international maritime trade moving through the Gulf of Aden is with Europe."[101] A large amount of oil shipped from the Middle East to North America travels through the Indian Ocean and around the Cape of Good Hope of South Africa. Thus, the Gulf of Aden and the Indian

[87] Massimo Annati, "Maritime Operations Off the HOA," *Naval Forces,* 1 (2010): 27.
[88] "Transforming National Security: AFRICOM--An Emerging Command Synopsis and Key Insights," *National Defense University*, February 19-20, 2008, *available at* www.ndu.edu/ctnsp/NCW_course/AFRICOM%20Summary%20Notes.pdf (March 17, 2008).
[89] Peter Spiegel, "Gates Says Somalia Government Is Key to Problem," *The Wall Street Journal,* April 14, 2009, *available at* http://online.wsj.com/article/SB123967368677815883.html.
[90] "The world's top consumers and producers of oil," *CNN*, June 3, 2008, *available at* http://www.cnn.com/2008/US/06/02/oil.map/index.html.
[91] Nick Brown, "T-72 main battle tanks finally unloaded from MV Faina," *Jane's Information Group*, February 17, 2009, *available at* http://www.janes.com/news/defence/land/idr/idr090217_1_n.shtml.
[92] Miller, 29-31.
[93] Mathew Weaver, "Timeline: Somali pirates attempted hijacking of Maersk Alabama cargo ship," *The Guardian* April 9, 2009, *available at* http://www.guardian.co.uk/world/2009/apr/09/somali-pirates-us-ship.
[94] "Maersk A-Class," *GlobalSecurity.org*, *available at* http://www.globalsecurity.org/military/systems/ship/maersk-a.htm.
[95] "Somaliland Anarchy in Somalia: The Lawless Horn."
[96] Muhammad Shamsaddin, "38 Days off the Somali Coast: MV FAINA Crisis Ecoterra 36th and 37th Updates," December 3, 2008, *available at* http://www.afroarticles.com/article-dashboard/Article/38-Days-off-the-Somali-Coast--MV-FAINA-Crisis-%E2%80%93-Ecoterra-36th-and-37th-Updates/142250.
[97] Astrid Tuminez, "Russian Nationalism and Vladimir Putin's Russia," *George Washington University*, *available at* www.gwu.edu/~ieresgwu/assets/docs/ponars/pm_0151.pdf.
[98] "Piracy off Somalia: Perils of the sea," *The Economist*, April 16, 2009, *available at* http://www.economist.com/node/13496719.
[99] Rawle O. King, 1.
[100] Ibid., 1, and *Countering Piracy Off the Horn of Africa: Partnership and Action Plan*, 4.
[101] "Economic Impact of Piracy in the Gulf of Aden on Global Trade," *US Department of Transportation Maritime Administration*, *available at* http://www.marad.dot.gov/documents/HOA_Economic%20Impact%20of%20Piracy.pdf.

Ocean are major sea lanes that allow for critical oil supplies to reach the Europe and United States.

Piracy is also a threat to Somalia and the region as a whole. One third of Somalia's population is fed by the United Nations World Food Program "90% of which are delivered by sea." Also potentially affected by piracy are the "inland markets in East and Central Africa that depend on imports from ports on the Indian Ocean."[102]

The majority of ships that pass through the Gulf of Aden and the Indian Ocean are not disturbed by pirates. For example, Lesley Anne Warner said that "In 2009, of the approximately thirty thousand vessels that pass through the Gulf of Aden every year, 217 were attacked. Of these, only forty-seven were successfully hijacked… only 0.72 percent of the ships that traversed the gulf were attacked in 2009."[103] Warner also said that "80 percent of attempted pirate attacks are foiled without assistance from warships," up from 60 percent in 2008.[104] It is unlikely that this will decrease the allure of piracy for Somalis. A country with an "urban unemployment rate… at 66% and the rural equivalent at 41%," needs more than lower success rates to discourage them.[105]

Thus, pirates are motivated by the ransom. Piracy offers high rewards and low risks. The pirates use violence in order to convince the targeted ship to stop, but rarely use violence after the hijack because the crew is part of the ransom. Piracy has been on the rise after the SCIC was removed from power in 2006; more alarming for the international community than the numbers of attacks are the potential targets. The Gulf of Aden and Indian Ocean allow the transport of critical oil shipments to Europe and North America. Successful hijackings such as the MV *Sirius Star*, the MV *Faina*, and the MV *Maersk Alabama* have shown that Somali pirates are willing to attack oil and arms shipments, and Middle Eastern, European, and American ships. Even though only a small percentage of ships are attacked, the attacks have a negative regional impact.

IV: Western Naval Response to Somali Piracy

Anti-piracy operations off the Horn of Africa began as an offshoot of anti-terrorism operations. After the terrorist attacks on September 11, 2001, CTF-150 was tasked with combating maritime terrorism.[106] In January 2009, the US Navy created CTF-151, a coalition task force devoted to conducting anti-piracy operations off the coast of Somalia.[107] In 2008 the EU created Operation Atatlanta, which was tasked with protecting shipping from Somali pirates.[108] NATO's contribution to anti-piracy, called Operation Ocean Shield, began August 12, 2009.[109] Independent powers such as Russia, China, and Iran have also participated in anti-piracy operations.

CTF-150 was forced to participate in anti-piracy operations as a result of the increase in Somali piracy.[110] It is not clear when CTF-150 began actively pursuing pirates, but the incident when the USS Winston S. Churchill DDG-81, captured a pirate ship on January 21, 2006, has been established as the first example of CTF-150's active anti-piracy operations.[111] However, the ship histories of the USS Oscar Austin DDG-79, USS Donald Cook DDG-75, and the USS Gonzalez DDG-66, prove that CTF-150's active anti-piracy operations were conducted in the third quarter of 2005. During its 2005-2006 deployment, the Oscar Austin served "as a deterrent for potential piracy operations," and on November 27, 2005, joined Operation Foresail. On September 21, 2005, the Gonzalez, "reported to the Horn of Africa in support of the Global War on Terrorism and anti-piracy operations," and the Gonzalez, continued anti-piracy operations until November.[112] The Oscar Austin's Visit, Board, Search, and Seizure (VBSS) team boarded the MV *Al Manara,* on January 24, 2006 in order to restore control of the ship to its crew[113] and the Donald Cook, participated in anti-piracy operations during the period of November 3-28.[114]

December 12, 2004, the German Frigate Mecklenburg-Vorpommern, which was assigned to CTF-150, sent a helicopter to defend a yacht that was attacked in the Gulf of Aden. The Mecklenburg-Vorpommern was conducting anti-terrorism operations at the time.[115] March 17, 2005 US Coast Guard Cutter Munro (WHEC-724), HMS Invincible R-05, and HMS Nottingham D-91, responded to a report of an act of piracy. The three ships acting under the CTF-150 command, arrested the pirates and restored control of the vessel to the ship's crew.[116]

CTF-151 was as a result of the rapid growth of Somali piracy in 2008. It is similar in structure to CTF-

[102] Warner, 67.
[103] Ibid., 65.
[104] Ibid., 69 and 73.
[105] Panjabi, 389.
[106] "Combined Task Force 150," *Naval Forces Central Command*, *available at* http://www.cusnc.navy.mil/cmf/150/index.html.
[107] "Combined Task Force 151," *Naval Forces Central Command*, *available at* http://www.cusnc.navy.mil/cmf/151/index.html.
[108] Miller, 60.
[109] "Operation Ocean Shield," *NATO, available at* http://www.manw.nato.int/page_operation_ocean_shield.
[110] Guy Toremans, "New Commander CTF-150," *Naval Forces,* 1.2009, 55-56.
[111] Miller, 55 and 65.
[112] "USS Gonzalez DDG-66 Ship History Report," *Washington Naval Yards, Ship History Archives*, Washington, D.C.
[113] "USS Oscar Austin DDG-79 Ship History Report," *Washington Naval Yards, Ship History Archives*, Washington, D.C.
[114] "USS Donald Cook DDG-75 Ship History Report," *Washington Naval Yards, Ship History Archives*, Washington. D.C.
[115] "Coalition Maritime Forces Deter Pirate Attack Off Yemen," *The U.S. Navy,* December 15, 2004, *available at* http://www.navy.mil/search/display.asp?story_id=16309, and Charles Dragonette, "Worldwide Threat to Shipping Mariner Warning Information," *Office of Naval Intelligence Civil Maritime Analysis Department,* December 22, 2004, *available at* http://www.nga.mil/MSISiteContent/StaticFiles/MISC/wwtts/wwtts_20041222000000.txt
[116] "Coalition Maritime Forces Intercept Hijacked Vessel," *The U.S. Navy*, March 18, 2005, *available at* http://www.navy.mil/search/display.asp?story_id=17550, and Charles Dragonette, "Worldwide Threat to Shipping Mariner Warning Information," *Office of Naval Intelligence Civil Maritime Analysis Department*, March 23, 2005, *available at* http://www.nga.mil/MSISiteContent/StaticFiles/MISC/wwtts/wwtts_20050323000000.txt.

150.[117] Ships assigned to CTF-151 are only responsible for conducting anti-piracy operations.

EU Naval Force Somalia Operation Atatlanta was created on November 11, 2008.[118] The EU created Operation Atatlanta in order to support the UN Security Council Resolutions 1814, 1816, 1838, and 1846.[119] Resolution 1816 authorized foreign navies to enter Somali territorial waters in order to conduct anti-piracy operations, with TFG permission, for a six month period.[120] Resolutions 1838 and 1846 extended the six month period.[121] NATO's Operation Ocean Shield, was created on August 17, 2009.[122] It looks to disrupt piracy off of the HOA in a similar manner to CTF-151, and Operation Atatlanta.[123]

US Navy

Between the various international anti-piracy operations there are roughly 30 ships patrolling the HOA, at any given time, and CTF-151 commands more than 20 of them.[124] The US Navy has committed amphibious landing ships, supply ships, cruisers, and destroyers to combat piracy. This may change in favor of smaller ships such as patrol craft, frigates,[125] and the Littoral Combat Ship (LCS).[126] Smaller ships do not suffer from the drawbacks that have sidelined them from traditional naval missions. A lack of offensive and defensive missile launch capability is not relevant when combating piracy.

Smaller ships are valuable in anti-piracy missions because they offer a cost effective presence. For example the maximum crew size of an LCS is 100 officers and enlisted,[127] the USS Ronald Reagan CVN-76, a carrier, can house over 6,000[128], and the destroyer USS Oscar Austin 380.[129] Thus, the crew of one destroyer could man three or four LCS's. The LCS is also relatively inexpensive. It costs $480 million, compared to the average cost to build a US Navy ship; estimates range from $2.1 to $2.7 billion.[130] Thus, for the same amount of money and manpower the US Navy can build and maintain four LCS's. Ships only have between 15-30 minutes to get help once attacked.[131] An anti-piracy force of numerous smaller, faster ships is more efficient than a smaller force of ships designed for fleet and land engagements because they could assist more pirated vessels.[132]

There have been two phases in the US Navy's anti-piracy mission. The first was preCTF-151 when the Navy used resources designed for other missions. The second phase began with the creation of CTF-151 when the US Navy altered its resources in order to adapt to the anti-piracy mission. A third phase may develop, if piracy continues, and would involve the US Navy designing its resources with anti-piracy as a primary mission.

Many of the changes that the US Navy has made in order to strengthen its Anti-Terrorism Force Protection have also made ships more effective at combating pirates.[133] Versatility is the key to the second phase weapons. The US Navy sees piracy as one of many missions and is slowly adapting its weapons to combat all of them. Examples of new systems that the US Navy brought online in order to fight piracy and other threats include: the GAU-17 7.62mm mini gun, the MK 49 Mod 0 remote controlled 12.7mm gun, MK38 Mod 2 25mm canon, and the MK15 Phalanx Close-In Weapon System Block 1B. By adding short range firepower the US Navy made ships more effective at fighting piracy.

The US Navy's VBSS teams are another example of adapting a resource that was designed for the Global War on Terrorism and converted for the anti-piracy mission. VBSS teams were designed in order to enforce UN Resolutions after the first Gulf War. After 9/11 the mission of a VBSS team was to "board ships in search of terrorists that utilize the world's oceans to traffic weapons and other contraband," and they have been used to combat piracy.[134]

---

[117] "Combined Task Force 151."

[118] "Javier SOLANA, EU HR, congratulates Cdre Antonios PAPAIOANNOU on his appointment as the EU Force Commander for OP ATALANTA," *European Union Naval Force Somalia - Operation Atalanta, available at* http://www.eunavfor.eu/2008/12/javier-solana-eu-hr-congratulates-cdre-antonios-papaioannou-on-his-appointment-as-the-eu-force-commander-for-op-atalanta/.

[119] "European Union Naval Force Somalia - Operation Atalanta," *European Union Naval Force Somalia*, *available at* http://www.eunavfor.eu/about-us/mission/.

[120] "United Nations Security Council Resolution 1816," *United Nations Security Council,* June 2, 2008, *available at* http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N08/361/77/PDF/N0836177.pdf?OpenElement.

[121] "United Nations Security Council Resolution 1838," *United Nations Security Council,* October 7, 2008. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N08/538/84/PDF/N0853884.pdf?OpenElement , and "United Nations Security Council Resolution 1846," *United Nations Security Council,* December 2, 2008, *available at* http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N08/630/29/PDF/N0863029.pdf?OpenElement.

[122] "Operation Ocean Shield."

[123] "NATO Warships Meet for Counter Piracy Mission Handover," *Headquarters Allied Maritime Command Northwood*, August 6, 2010, *available at* http://www.manw.nato.int/pdf/Press%20Releases%202010/Jun%20-%20Dec%202010/SNMG1/SNMG1%202010%2017.pdf , and "NATO Warship HMS Montrose Races To Assist Ship After Pirate Attack," *Headquarters Allied Maritime Command Northwood*, *available at* http://www.manw.nato.int/pdf/Press%20Releases%202010/Jun%20-%20Dec%202010/SNMG1/SNMG1%202010%2029.pdf.

[124] Warner, 72 and Ploch, 22.

[125] Kreisher, 6.

[126] Martin Murphy, "Littoral Combat Ship," *Center for Strategic and Budgetary Analysis*, 66.

[127] Ibid, 17.

[128] "USS RONALD REAGAN," *Naval Vessel Registry, available at* http://www.nvr.navy.mil/nvrships/details/CVN76.htm.

[129] Oscar Austin," *Naval Vessel Registry*, *available at* http://www.nvr.navy.mil/nvrships/details/DDG79.htm.

[130] "The Long-Term Outlook for the U.S. Navy's Fleet," *Congressional Budget Office*, January 20, 2010, 7-10.

[131] Ploch, 12.

[132] Murphy, "Suppression of Piracy and Maritime Terrorism," 37.

[133] Massimo Annati, "Weapons Optimised for Anti-Terrorist and Anti-Pirate Operations," *Naval Forces,* 2.2008, 55.

[134] Ed Barker, "VBSS: Evolving with the Mission," *GlobalSecurity.org*, April 4, 2009, *available at* http://www.globalsecurity.org/military/library/news/2009/04/mil-090425-nns05.htm, and Andrew King, "Nassau Creates VBSS

VBSS teams are trained to participate in Maritime Interdiction Operations, traditionally anti-terrorism and anti-smuggling operations. They are taught to board vessels from Rigid Hull Inflatable Boats (RHIB) with telescopic poles and metal ladders. A RHIB is lowered from a ship into the water and the VBSS team uses it to board suspicious vessels. VBSS teams, with the exception of Special Forces, are not trained in school for anti-piracy operations.[135]

The US government developed specific goals in order to prevent Somali piracy attacks in the Gulf of Aden and the Indian Ocean. Secretary of State Hillary Clinton announced four steps to fight piracy. The first is for ship owners to stop paying ransoms, second an expanded multinational response which includes attacking pirate assets, third pressuring the leaders of Puntland and the TFG to combat piracy within their borders, and fourth build ship self defense capabilities.[136] The NSC recommended three steps and the first was to "prevent pirate attacks by reducing the vulnerability of the maritime domain to piracy," second to "interrupt and terminate acts of piracy," and third to "ensure that those who commit acts of piracy are held accountable for their actions by facilitating the prosecution of suspected pirates."[137] A summary of US antipiracy policy was Lesley Warner's identification of

> Eight counterpiracy methods… in use or under consideration by the United States:
> - Accepting piracy as a cost of doing business
> - Tracing and targeting pirate finances
> - Increasing the defenses of merchant vessels
> - Address legal impediments to combating piracy
> - Continuing multinational naval patrols
> - Pursuing kinetic operations on land
> - Building local and regional maritime security-sector capacity
> - Building local and regional security-sector capacity on land.[138]

She concluded that it would not be possible to ignore Somali piracy because of the commerce that transits through the Gulf of Aden. The cash-based Somali economy makes tracing the pirates' finances impractical. Increasing the defensive capabilities of merchant ships succeeded in making them harder targets, at the price of higher shipping costs. Naval patrols reduce the success rate of piracy, not eliminate it. US military will not pursue pirates on land. Progress has been made in building local navy's anti-piracy operations, but any major impact would be in the future. Finally, local efforts on land were counterproductive.[139]

US policy makers, such as former Secretary of State Condoleezza Rice, acknowledge "that maritime operations alone are insufficient."[140] This is the limitation of the US anti-piracy policy; it only attacks piracy at sea. Support for the TFG has not produced tangible results and the US is unwilling to commit troops on land in Somalia while engaged in wars in Iraq and Afghanistan. With new weapons, the maritime operations may become more effective, but they will not be able to stop piracy. President Barrack Obama articulated his position on Somalia when he said that

> Imposing peace from the outside through military force or coercion is not a recipe for success… Life under colonialism is still well remembered and leaves a bitter aftertaste. Instead, keeping the hotspots cool is better left to the Africans, although they need assistance in the form of training and equipping their military peacekeeping units.[141]

America will help Somalis help themselves, but there will not be another Operation Restore Hope under the Obama administration.

The Smaller the Better

If the piracy problem is left to the Somali people to deal with, it is possible that pirates will be attacking shipping in the Gulf of Aden and the Indian Ocean for the foreseeable future. It is also possible that unstable nations near other shipping routes will develop pirate networks. It is expensive for foreign navies to keep ships deployed off the coast of Somalia. Fast Attack Craft (FAC) could help protect shipping at a fraction of the cost it takes to deploy larger ships. If the US and the UN are unwilling, or unable, to restore stability to Somalia the responsibility falls on the AU. Thus, FAC and operations such as AU Mission in Somalia (AMISOM) may be economical options to reduce, if not remove, the threat of piracy.

It could take a force three times the size of the US Navy to protect all ships that pass through waters that are affected by Somali Pirates.[142] In order to stop piracy in the Gulf of Aden alone, it will take a task force of

---

Team," *USS Nassau Public Affairs*, February 14, 2007, *available at* http://www.navy.mil/search/display.asp?story_id=27783.

[135] "Maritime Interdiction Operations (MIO)," *Recce Group*. *available at* www.reccegroup.com/Recce%20Group_Course_Maritime%20Interdiction%20Operations.pdf, *see also* "Statement of Work for Instructional Support in the West Region For Navy Security Forces Training Under the Direction of the Center for Security Services," *US Navy*, *available at* cryptome.quintessenz.at/mirror/dodi/navsec-sow.pdf, *see also* "Training Course Control Document for Visit, Board, Search, & Seizure (VBSS) Team Mechanical Breacher Mechbreachervbss," *NAVAIR Orlando Training Systems Division*, *available at* https://www.neco.navy.mil/necoattach/N0018910R0064Attachment_C_TCCD_for_VBSS_Breacher.pdf, and *see also* "TRAINING COURSE CONTROL DOCUMENT FOR NON-COMPLIANT BOARDING, VISIT, BOARD, SEARCH AND SEIZURE (NCB-VBSS) TEAM TRAINER **A-830-0395** (REVISION A)," *Center for Security Services (CENSECFOR),* June 30, 2008.

[136] Hillary Rodham Clinton, "Announcement of Counter-Piracy Initiatives," *U.S. Department of State*, April 15, 2009, Washington DC, *available at* http://wwwstate.gov/secretary/rm/2009a/04/121758.htm.

[137] "Countering Piracy Off the Horn of Africa: Partnership & Action Plan," 7-12.

[138] Warner, 65.

[139] Ibid., 65-79.

[140] Condoleezza Rice, "Combating the Scourge of Piracy," Speech, *United Nations Security Council*, December 16, 2008, New York, New York, http://merln.ndu.edu/archivepdf/AF/State/113269.pdf.

[141] William E. Ward, and Thomas P. Galvin, "Africa's Future Is Up to Africans," *Joint Force Quarterly*, 58 3rd Quarter, 2010, 7-8.

[142] Warner, 74.

around 60 combat ships. The Indian Ocean is much larger and would require a bigger force.[143] Thus it is possible to stop piracy in the Gulf of Aden if the multi-national effort were reinforced; however this would cause the pirates to shift their operations into the Indian Ocean. This would have a negative impact on the nations that ship goods on the Indian Ocean, and in particular the South Eastern region of Africa.

FAC will not solve the piracy problem by increasing the number of ships off the HOA. They can make it more difficult for pirates to operate in coastal areas such as the Red Sea and the Gulf of Aden, and they allow smaller maritime nations that lack the resources of the traditional western powers, to protect their shipping. FAC are preferable in coastal anti-piracy operations because they are faster, cheaper, require less upkeep, and "the heavier armament of a frigate provides little advantage," when fighting pirates.[144] By comparing the Norwegian *Fridtjof Nansen* class frigate and the Norwegian *Skjold* class FAC the advantages of the FAC are evident. The frigate costs $600 million, more than half a billion dollars than the $65 million for the *Skjold* class FAC. The frigate has a crew of 120 and the FAC a crew of 15.[145] The top speed of the frigate is 27 knots and the FAC has a top speed of 55+ knots.[146] The American Oliver Hazard Perry class frigates are often sold, or given, to allied navies after they have been decommissioned by the US Navy.[147] The refurbished American frigates can have a crew of over 200 sailors and a top speed of 29 knots.[148] The *Skjold* class FACs are superior to their larger brethren when fighting piracy; they are cheaper, faster, and require a much smaller crew compliment. Frigates are not as well suited for anti-piracy operations due to their large crew and slower speed, even if they are free. For countries that cannot afford the $65 million price tag India and China have built FACs that cost less than $15 million.[149] Thus at a fraction of the price of a larger ship FACs provide a viable alternative for countries that need to protect their shipping, but have a limited budget and a shortage of trained personnel.

AMISOM lost the good will of the Somali people due to charges of AU troops of killing civilians.[150] Opinions can change with time if the presence of the AU soldiers produces tangible benefits for Somalia. President Obama was correct that another US or UN peacekeeping mission would have probably been seen as a neocolonialist invasion. The US is better served by providing logistical support for AMISOM, which it has done by providing more than $160 million worth of services and equipment.[151] Despite this, the international effort had not given the AU the resources it required to accomplish its mission in Somalia.[152] A land solution to the piracy problem is the best option because the only decrease in piracy activity came as a result of the SCIC's dominance in southern Somalia. With that in mind, if the AU troops were well trained and supplied, and came in large enough numbers they should be able to temporarily impose stability. The situation is complicated by clan loyalties and factions, but it is not AMISOM's mission to rule Somalia, only to give the TFG a chance to do so.[153]

Private Security on Merchant Ships and the Impact of Piracy on Shipping Costs

Merchant vessels should implement more efficient methods of defending themselves against pirate attacks. There have been developments in this field that lower the probability that pirates will successfully board ships; however, they raise the cost of transport. The ONI identified five key threat factors weather, merchant ship speed, the time of day, expanded attacks in the Indian Ocean, and how targets were selected. They found that weather was the most important factor that determined when pirates attack. Ships were safer during the two monsoon seasons, at night, and when traveling at high speeds. Pirates were operating deeper into the Indian Ocean as a result of increased patrols in the Gulf of Aden, and there was no indication of pirates having been informed of ship's routes; victims were targets of opportunity.[154]

Convoys have been implemented in the Gulf of Aden in order to protect shipping. The Internationally Recognized Transit Corridor (IRTC) has helped reduce the success rate of pirate attacks in the Gulf of Aden.[155] The IRTC allows warships to protect large numbers of merchants by grouping them together, and ships help protect each other. Convoys slow down shipping which results in a loss of money for shipping companies, and it

[143] Ploch, 13.
[144] Friedman, Norman, "Countering the Pirate and Terrorist Threat," *Naval Forces,* 27.5, 2006, 83-84.
[145] "Norway's New Nansen Class Frigates: Capabilities and Controversies," *Defense Industry Daily*. *available at* http://www.defenseindustrydaily.com/norways-new-nansen-class-frigates-capabilities-and-controversies-02329/; and *see also* "The Skjold Class Fast Reaction Craft," *Umoe Mandal*, 2000, *available at* http://www.foils.org/skjold%20brief.pdf.
[146] "Fridtjof Nansen (F85) class PROJECT 6088 NEW FRIGATE," *GlobalSecurity.org*, *available at* http://www.globalsecurity.org/military/world/europe/nansen.htm; and *see also* Arthur G. Self, "Fast Attack Craft (FAC) and Their Roles," *Naval Forces*, 1, 2010, 17.
[147] "Pak to get $65 million US warship free of cost," *The Indian Express, available at* http://www.indianexpress.com/news/pak-to-get-65-million-us-warship-free-of-c/611941.
[148] "USS Ingraham," *Naval Vessel Registry*, *available at* http://www.nvr.navy.mil/nvrships/details/FFG61.htm; and *see also* "FFG-7 Oliver Hazard Perry Class," *GlobalSecurity.org*, *available at* http://www.globalsecurity.org/military/systems/ship/ffg-7.htm.
[149] Self, 22.
[150] Warner, 79.
[151] Ploch, 3.
[152] Warner, 78-79
[153] "UN Security Council Resolution 1772," *United Nations Security Council,* August 20, 2007, *available at* http://www.un.org/Docs/sc/unsc_resolutions07.htm.
[154] "Horn of Africa: Threat Factors for Commercial Shipping and Forecast of Pirate Activity Through 2009."
[155] Marieke J. Rietveld, "Piracy Considerations on Passage of the Gulf of Aden and/or the North West Indian Ocean East of Africa," *Royal Netherlands Institute for Sea Research*, *available at* http://www.eurocean.org/np4/file/863/Piracy_Gulf_of_Aden__Indian_Ocean.pdf.

is possible that the lost revenue costs more than the ransom payments.[156]

In order to defend ships, crews have increased surveillance in order to detect attacks sooner, rehearsed lock down methods to prevent pirates from accessing the crew, barbed wire and electric fences, and the increased use of nonlethal devices such as fire-hoses, and long-range acoustic devices (LRAD) have successfully prevented boarding's, as have Molotov cocktails and covering decks with broken glass.[157] Though these techniques have been successful pirates may be adapting to them, in which case more violent methods may be required for crews to defend themselves.[158]

There has been rising support for merchant ships to arm themselves in order to fight pirates; however, it could complicate the situation. For example, crews are not trained in firearms safety or marksmanship, some ports do not allow armed ships to dock, security teams are expensive, armed ships could increase the threat of terrorism, and gun battles would escalate the violence. Despite the drawbacks, the US has embarked security teams on ships that carry military supplies off the HOA.[159] Armed crews may be necessary for critical shipments such military hardware and energy, but are not cost effective for other shipments.

The cost of insurance to ship products through the Gulf of Aden has increased due to piracy. Cost to insure a container rose from $900 to $9,000 and war-risk insurance may increase the cost of insuring a ship between $10,000 and $20,000 per trip. Options to avoid the Gulf of Aden also increase the cost of shipping. If a merchant ship reroutes around the Cape of Good Hope it adds nearly 3,000 miles to the trip. This increases operating costs and reduces the number of deliveries the ship can make. An estimate of the increased costs merchants face due to piracy is $60,000 for a security guard per trip through the Gulf of Aden, $20,000 to $30,000 for an LRAD and an operator, or $3.5 million in fuel annually to reroute a ship around the Cape of Good Hope.[160] Merchant ships can mitigate the risks associated with piracy, but it is impossible to remove the risk without raising the cost of shipping.

Catch and Release

Despite international law that gives any country that apprehends a pirate the right to prosecute, most do not.[161] The Danish Navy released pirates even though they found evidence of pirate activity, which included weapons and plans to divide the ransom with Somali warlords.[162] Some progress has been made making it easier for countries to prosecute pirates, but most only prosecute pirates they catch in the act of piracy, or pirates that attacked a ship from their country.[163] The West does not want to prosecute pirates for reasons that range from expense to possibly having to grant pirates immigrant status at the end of their prison term. In order to avoid prosecuting pirates in Europe or America, the EU, UK, and US, made arrangements with Kenya, to prosecute them.[164] The Seychelles have also agreed to prosecute pirates, but the small nation has a very limited prison capacity. Both Kenya and the Seychelles have been given money to update their justice systems in order to deal with the increased number of prisoners and court cases. However, Kenya has voiced reluctance to become a dumping ground for pirates without the West sharing the burden.[165]

The lack of enthusiasm for prosecution is an indication of the West's desire to ignore the growing problem. It looks as though the US and Europe are willing to send their ships to fight piracy as long as they do not have anything more important for them to do, but when it comes to making a long term commitment there is a reluctance. With the Somali economy in a disastrous state there is a financial incentive for Somali men to turn to piracy. Prison sentences will not eliminate Somali piracy, but large scale prosecution would be one element in a multi-pronged strategy to discourage the growing trend.

Conclusion

The Western response has shown a reluctance to combat piracy in a realistic manner. This is due to a desire to fight pirates as though they were terrorists, and a lack of follow up that degraded mission effectiveness. Somali pirates are not terrorists; they have no proven links to terrorist networks, nor are they interlopers from the past armed with cutlasses and muskets. Somali pirates are dangerous, but they do not threaten Western society. The threat is first regional and second global. Pirate attacks in the Gulf of Aden and the Indian Ocean have had a destabilizing effect on the East African region. By hijacking arms, and food aid shipments, pirates have the ability to alter the balance of power, and increase the risk of famine, in a region that is fraught with instability and starvation. The global threat is primarily commercial with increased shipping costs as the likely result. However, critical supplies that are

[156] Ploch, 36-37.
[157] Ibid., 34; Warner, 68-69, Stehr, "Modern Piracy: Growing Threat to Shipping, Counter Threat Technology and Tactics," 26-31; and Axe, "10 Things You Don't Know About Somali Pirates."
[158] "Piracy and Private Enterprise."
[159] Ploch, 34-35, and Warner 69-70.
[160] "Economic Impact of Piracy in the Gulf of Aden on Global Trade."
[161] Ploch, 31-33, and James P. Terry, "Eliminating High Seas Piracy: Legal and Policy Considerations," *Joint Force Quarterly,* 54, (3rd Quarter 2009).
[162] Paulo Prada, and Alex Roth, "On the Lawless Seas, It's Not Easy Putting Somali Pirates in the Dock," *The Wall Street Journal,* December 12, 2008, *available at* http://online.wsj.com/article/SB122903542171799663.html.
[163] "Piracy Wong Signals," *The Economist,* May 7, 2009, *available at* http://www.economist.com/node/13610785/print.
[164] Panjabi, 481-84.
[165] Warner, 71-72; and Michael Onyiego, "Seychelles to Establish Regional Court to Prosecute Pirates," *VOA*, May 6, 2010, *available at* http://www.voanews.com/english/news/Seychelles-to-Establish-Regional-Court-to-Prosecute-Pirates-92969969.html.

shipped through these sea lanes are vulnerable, and could adversely impact dependent economies.

The international community has shown an inconsistent approach to anti-piracy operations. Catch and release and the unwillingness of Western nations to support a stable government in Somaliland are troubling. The TFG has been unable to govern Somalia, and for a period of time it was forced into exile in Kenya, yet the US continues to support this "government." Ousting the SCIC was another example of the US showing a lack of commitment to the anti-piracy mission. The US decided to favor its battle with Islamic fundamentalists and overthrew the one government that had effectively reduced piracy off the HOA.

There is no cure for Somali piracy, short of a stable government in Somalia. The US refuses to take the steps necessary to ensure that the TFG has the time necessary to establish a functional government. This is due in part to the two land wars that the US is involved in, and the disastrous outcome of Operation Restore Hope. The AU mission in Somalia, AMISOM, is an alternative to a Western, neocolonial peacekeeping mission. If AMISOM were properly manned, equipped, and funded the TFG could have a fighting chance to control Mogadishu and reclaim territory from the Shabab Militia. If the US lent support to Somaliland, Puntland, and the TFG, with AMISOM assistance, in return for anti-piracy measures, piracy would decline. It is the safe haven on land that allows piracy to flourish; if the pirates were attacked on land as well as at sea it would be a less lucrative profession.

Prosecuting pirates is necessary in order to create a deterrent to committing acts of piracy. Releasing pirates shows a lack of commitment to the anti-piracy mission and is a signal to pirates that there are no consequences. There are, however, economic motivations for Somali fishermen to turn to piracy. The ravaged Somali economy offers few economic opportunities as promising as the piracy.

The US Navy, and its European counterparts, could increase the efficiency of their anti-piracy operations as well. If the US evolved from the second stage of anti-piracy operations into the third stage, which involves ships and equipment designed for anti-piracy, it could increase its ability to protect shipping. More, smaller ships would have a profound impact on the international task forces' ability to be in more places at the same time, which is a key to interrupting pirate attacks.

Arming ships that transport critical supplies would reduce the threat of those shipments being successfully hijacked. It is not advisable to arm all ships that travel through the HOA, but there are steps that all ships can take to decrease the rate of successful hijackings. Passive defenses such as barbed wire, combined with updated and rehearsed security plans would make merchants harder targets. Travelling at night and during the monsoon seasons would also reduce the likelihood of attack.

Somali piracy will continue to be a threat for years to come; if and when it ends, piracy will most likely develop somewhere else. That is why it is important that the US and Europe, develop mechanisms in order to prosecute pirates, and their navies develop the tools necessary to combat pirates at sea. With the creation of CTF 151, Operation Atatlanta, and Operation Ocean Shield the naval effort has made steps in the right direction, but there is more to be done. Piracy can threaten critical supplies and destabilize regions. If globalization is the cause of piracy, this is a threat that will be around for the foreseeable future. It is for this reason that world powers should use this opportunity to learn what they can on how to best fight piracy.

Cyber-terrorism

Jack Jarmon

The Internet is a critical infrastructure necessary to the functioning of commerce government and personal communication and national security. The system is not secure. – Intelligence and National Security Alliance report, November 2009

In a 2002 report prepared by the Center for Strategic and International Studies (CSIS), Jim Lewis, a former official with the Department of State and the Department of Commerce wrote:

> The idea that hackers are going to bring the nation to its knees is too far-fetched a scenario to be taken seriously. Nations are more robust than the early analysts of cyberterrorism and cyber warfare gave them credit for. Infrastructure systems [are] more flexible and responsive in restoring service than the early analysts realized, in part because they have to deal with failure on a routine basis.[1]

Six years later, in its 2008 report, *Securing Cyberspace for the 44th Presidency*, the same CSIS concluded:

> Cybersecurity is among the most serious economic and national security challenges we face in the twenty-first century. Our investigations and interviews for this report made it clear we are in a long-term struggle with criminals, foreign intelligence agencies, militaries, and others with whom we are intimately and unavoidably connected through a global digital network; and this struggle does more real damage every day to the economic health and national security of the United States than any other threat. As one general put it in his briefing to us: *In cyberspace, the war has begun.*

Interestingly, the project director for the 2008 report was, again, Jim Lewis. The contrast of analysis is not only striking for its reversal of positions, but also in its tone. The 2008 report called for a profound reorganization of our national defenses that embraces a spirit of partnership between the US Government, its allies, and the private sector. It also urges a break with the past on issues of de-regulation, security classification, and the call for leadership in order to drive forward a comprehensive cybersecurity strategy. The authors also concede that the information age has forced us to re-think how federal government operates across boundaries within and outside itself.[2]

How such previous attitudes could have been overturned so radically in a relatively brief span of time reveals more about the dynamic of the information-communication technology (ICT) revolution rather than it does about errors in a particular expert's analysis. Not only the pace of technology but also the rate of growth and expansion of critical infrastructures, such as government, finance, energy, etc., have intensified our society's use and dependency upon ICT.

In cyberspace, the war has begun

What, then, is cyberspace? Metaphorically, it is the realm of computer transactions. Physically, it is the hardware, software, and transport elements that equate to the network architectures through which energy passes delivering information. However, less specific or technical - but as unerring, is the definition by the science-fiction novelist William Gibson who first introduced the term. In his 1984 book *Neuromancer*, he expresses cyberspace as a "consensual hallucination. …A graphic representation of data abstracted from the banks of every computer in the human system." Although both definitions can be considered true, for the purposes of this book the definition offered by the U.S. Joint Chiefs of Staff is the most appropriate for the following discussion:

> A domain characterized by the use of electronics and the electromagnetic spectrum* to store, modify, and exchange data via networked systems and associated physical infrastructure.[3]

This strategic definition, rather than Gibson's "hallucination," allows us to discuss cyberspace and attendant concepts with the same terms that we use to understand and express our notions about the oceans, the ecosystem, outer space, or other frontiers of human endeavor where serious challenges co-exist alongside opportunities for cooperation. However, to have a basic grasp of those concepts and terms, we need to devote some time and explanation to clarifying the elements and scientific principles that make comprehension of the current information/communication system possible. Also, such familiarity with the facts gives us a sense of the system's fragility and our own national vulnerability.

An understanding of cyberspace begins with an understanding of telecommunications. In cyberspace circuits, or routes, that information travels can be physical (copper wiring, optical cable) or radiation based (microwave, WiFi). Vulnerability to attack is a feature of the transmission medium. Physical connections are subject to tapping and severed connections. Radiation based connections can be disrupted from broadcasted electro-magnetic signals. Walter Morris, Computing

[1] "Cyberterrorism: How Real is the Threat," United States Institute of Peace, December 2004

[2] "Securing Cyberspace for the 44th Presidency," Center for Strategic and International Studies Commission Report, Washington, December 2008, p. 78

* What is known as the electromagnetic spectrum is the combination of electric and magnetic fields. The reciprocal relationship between electricity and magnetism form the medium. When these forces are unified mathematically they create electromagnetic (EM) waves of radio and light. The oscillation of atomic interaction determines wave frequencies, which govern over such properties as visibility, energy, and can create the separate pathways, or wavelengths, along which information streams.

[3] Yannakogeorgos, Panayotis, *Technologies of Militarization and Security in Cyberspace*, doctoral dissertation, Rutgers University, April 2009, p. 28

Manager at Rutgers University, offers a wide-angle perspective on the domain of telecommunications:

> While cyberspace refers to a non-physical abstraction, it is achieved using computers networked via various means of communication. Information is exchanged between the nodes on a network in numerous ways, some physically connected and some using various radio transmitters/receivers.

Whether physically connected or radio transmitted, the integrity and security of these circuits are vested in the communication system's ability to redirect traffic to alternative pathways in the event of circuit failure. Whether a copper-based, wireless, or optical data transport environment, a network is resilient to outside physical attack and disruption due to this fundamental element - redundancy. A simple but significant feature, redundancy merely refers to the multiple paths by which information flows. As stated above, those multiple pathways can be copper wiring, radio frequency, or optical fiber. As long as communication flow has a reliable and alternate (redundant) route, the circulation of information continues as a matter of routine.

The material elements of these paths made little difference in the original scheme. The ability to withstand an intentional or natural onslaught and maintain operational stability by diverting a signal to an alternative routing system was the only concern in the early design, and is still the major concern today. What has changed is the growth of these networks, the volume of information transmitted, the threat vector, and our struggle to adapt to a new and perilous environment. These changes arose from the natural and irresistible forces of technological development and advancement.

Once optical cable made possible the transport of high volumes of data at the speed of light, the growth in optical fiber networks over copper cable systems surged robustly and irreversibly. The change over in technology set loose immense growth in the capacity and efficiency of I/C networks. It also unleashed a dependence on electronic networks, which is nothing less than a systemic addiction. Although optical fiber cannot yet replace copper in every instance, its impact on telecommunications has been momentous and incontrovertible. In a frequently used metaphor, wavelengths of light are the traffic lanes, which information travels along the information highway. When lanes become inaccessible or over-burdened with data, we use alternative routes by switching lanes or adding more. Adding more lanes, or in other words, widening the bandwidth was the solution and one of the drivers of investment craze of the late nineties. It, also, may have been a contributing factor to the over-investment and eventual implosion of the telecommunication industry.

What, exactly then, is it that streams along the information highway? In most transport forms, electronic messages are disaggregated into bits of data at the origin point - contained and sent in the form of small packets that have routing information in what is called a packet header. Routers along the network read the packet headers and relay the packets toward their destination. At the destination point the data is re-assembled as packets arrive to form the original message. A breakdown or interruption of transmission any place along the network will not cause a system failure. The data packets will simply be rerouted. Unless messages are encrypted or transmitted over virtual private networks (VPNs), information flows according to this mode of transport. The system's openness contributes to this resiliency as well as its vulnerability. VPNs are often considered more secure. However, as opposed to a packet routing system, if a message is intercepted at a point within a VPN or an encryption decoded before it reaches its destination, the message can be revealed and security is compromised.

The data packet system relies upon standardized communication protocols to assure operation and control. The Transmission Control Protocol/Internet Protocol (TCP/IP) is the common set of protocols (the rules governing the transmission of data between devices) invented in the early stages of development, and used today to form the global system of interconnected networks. It is the military grade protocol suite that transports packets of information between devices and throughout the network as it verifies correct delivery between servers. By reading the IP header, a routing device can determine the source and destination of each packet. The critical information in the IP header allows the transport layer of the TCP/IP, or "protocol stack" to operate across networks. The IP header is simply a string of numbers that machines, such as routers, read to direct packets toward their destinations and, hence, form connections. At the receiving end, the header carries information that also instructs the destination computer how to recreate the message from the incoming packet data.

These strings of numbers, by which machines communicate, are translated into letters by the Domain Name System (DNS) for easier understanding by humans. Therefore, rather than having to type 66.249.90.104 when accessing a search engine, you can enter the more user friendly Uniform Resource Locator (URL): 'google.com'. Thirteen root servers house the DNS databases, which facilitate translation between IPs and URLs. The former U.S. Department of Commerce agency, Internet Corporation for Assigned Names and Numbers (ICANN), allocates top-level designations such as com, org, edu, and so on, and maintains and updates the data. ICANN is now a private entity, and as a result of international pressure, has recently facilitated the movement from a less English-centric system of domain naming to accommodate other languages. The policy shift is a modest signal that there may be progress away from a U.S. - dominated Internet toward a spirit of international cooperation and a truly global public good.

The Inception of Cyberspace

In 1968 the Advanced Research Projects Agency (ARPA), which later became the Defense Advanced Research Projects Agency (DARPA), began work on what

would later become the modern day Internet. The project's goal was to invent a communications network, which could sustain physical attacks and survive malfunctions occurring at other points along the system. ARPAnet, as it was called, required a minimum level of security because the number of users were, initially small, trusted, and known to one another. Shortly after the inception of ARPAnet, the National Science Foundation (NSF) realized the potential impact this technology could have on university research. Unfortunately, to have access to ARPAnet an institution had to have a research contract with the Department of Defense. The disadvantage of having no contractual relationship with DoD put many universities outside the circle, or circuit, of research and information sharing. Under such conditions the full potential of these new skills and equipment would not be met.

In order to provide an apparatus to keep pace with the technology, the NSF created a successor system called NSFNET. NSFNET linked to ARPnet with a backbone network, which employed TCP/IP. From the start NSFNET was an instantaneous success and within a short time, became overloaded. The NSF realized it could not continue financing the build out indefinitely and, therefore, set plans for its commercialization.[4] By the 1990s companies called Internet Services Providers (ISPs) overtook an Internet, which previously had been dominated by government, university, and industrial researchers. These ISPs competed in regional areas based upon price and quality of service, and in the process signed up millions of customers. As Andrew Tannenbaum remarks in his seminal work, Computer Networks:

> Many people like to criticize the Federal Government for not being innovative, but in the area of networking, it was the DoD and the NSF that created the infrastructure that formed the basis of the Internet and then handed it over to industry to operate.[5]

As the modern Internet grew beyond its original, conceptual boundaries, features such as the capability to have voice communication or Voice over Internet Protocol (VoIP) were added. This made it increasingly depended upon the Public Telecommunications Network (PTN). The expanding interdependency between PTN and the Internet further elevates the risk of infrastructure vulnerability.[6] Since PTN has become more software driven, our reliance on computer networks has intensified. Increased usage demanded a need for larger scale of operations and resulted in the creation of more access points.

At its inception as a U.S. military project the Internet's security concerns were minimal. It was an open system because it was closed to others outside its small circle of users with authorized access to specific government-owned and sponsored large mainframe computers. Due to the government's original intension to keep the function and system limited and proprietary, much of the security issues we face today are inherited traits of a previous generation of development.

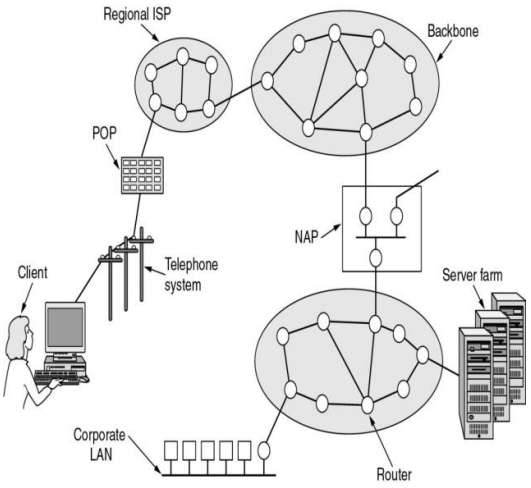
Today the Department of Defense, alone, has 15,000 computer networks and seven million computers and other network devices. DoD withstands more than three million log-ons each day.[7] For the above reasons TCP/IP, which lacks even base security controls, is perilously outdated.[8] It is from this design of over thirty-five years ago that the current network of connection support between autonomous systems and domain name services depends. Therefore, the Internet is inadequately secure by these current communication protocols. Despite our good intensions, in the haste to maximize its utility we have sacrificed resiliency and imperiled the stability of the many networks, upon which we so dearly depend. As if conceding these points, among its defensive strategy recommendations, the National Research Council goes as far as to urge: "Minimal exposure to the Internet, which is inherently insecure."[9] As a result of several top-level meetings (and, perhaps, in response to the NRC's recommendation) the Bush White House launched its National Cybersecurity Initiative (CNSI) during the waning days of its administration. The "cyber-initiative" included a dramatic re-scaling of the points at which federal networks connect with the Internet. The Office of Management and Budget set a limitation of 50 "points of presence" by June 2008. However, in March 2008, then Homeland Security Secretary, Michael Chertoff remarked: "we have no final number yet," with respect to a survey of all "points of presence."[10] According to Bruce McConnell, former chief of information technology and policy at the Office of Management and Budget, "Trying to catalog where things are so you can turn them off is a daunting task in and of itself."[11]

[4] Tannenbaum, Andrew, Computer Networks, Prentice Hall PTR, Upper Saddle River, NJ, fourth edition, 2003, p. 56-8
[5] Ibid, p. 56
[6] Nasheri, Hedieh, Economic Espionage And Industrial Spying, Cambridge University Press, 2005, p. 98

[7] Lynn, William, Deputy Secretary of Defense, in "US Creates Military Cyber Command to Defend Computer Networks," *Global Security*, 15 June 2009
[8] Hancock, Bill, "How to Stop Talking About-And Start Fixing cyber Security Problems," Cutter IT Journal (May 2006), in Yannakogeorgos, p. 212
[9] Making the Nation Safer: The Role of Science and Technology in Countering Terrorism, National Research Council of the National Academies, The National Academies Press, Washington, D.C., 2002, p.150
[10] Harris, Shane, "China's Cyber Militia" in *National Journal Magazine*, May 31, 2008, http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php
[11] Ibid

INTERNET ARCHITECTURE

Source: Computer Networks, Prentice Hall, 2003



In the view of the above assessments, our present security challenges are unmet. No longer a closed research project, but rather a global public good, the architecture suffers from host of vulnerabilities. A report released on May 29th, 2009 by the Acting Senior Director for Cyberspace assessed the information and communication infrastructure as thus:

> Without major advances in the security of these systems or significant change in how they are constructed or operated, it is doubtful that the United States can protect itself from the growing threat of cybercrime and state-sponsored intrusions and operations. Our digital infrastructure has already suffered intrusions that have allowed criminals to steal hundreds of millions of dollars and nation-states and other entities to steal intellectual property and sensitive military information. Other intrusions threaten to damage portions of our critical infrastructure. These and other risks have the potential to undermine the Nation's confidence in the information systems that underlie our economic and national security interests.[12]

In the absence of a major upgrade in system security the approach to security has been a "patchwork of niche products and work-arounds."[13] Such methods are responsible for many analysts claiming that security will always be a step behind attackers.[14] As Melissa Hathaway, lead member of the team, which prepared the 60-Day Cyberspace Policy Review for President Obama, stated:

> … our technical defenses have not kept pace with the threat, and it remains easier today – and I suspect for some time to come – for our adversaries to create an offense than for us to create a defense.

The April 2009 Cyberspace Policy Review Report and others have also called for a national comprehensive strategy that includes codes and best practices standards. Until these situations are addressed, the conclusions, doubts, and fears expressed above will remain.

Unfortunately, the barriers to amending the prevailing security environment are severely challenging to national governments and international commerce. The private sector primarily owns the electronic infrastructure, making security a business decision. In order to meet the demands of global commerce, corporate strategists are forced to favor their revenue generating units over investment in security. As long as the threat of catastrophe remains only an abstract fear, corporate boards will continue to view their responsibilities as vested in creating and accumulating assets, while leaving to subordinates the job of protecting those assets.

Equally unfortunate is that the public sector often takes its cues from the private sector. Deregulation of the telecommunications industry by obliging legislation and government agencies has over time helped to accelerate the growth of the Internet. Subsequently, the increased in the number of networks and access points only increases the opportunity and odds for an attack. This lack of regulatory oversight has had its impact on security. The lack of benchmarks to uphold security standards and the failure to create any incentives for industry to seriously self-regulate has consequences for national security. With only market incentive to drive the demand for improved and secure protocols, even existing methods and approaches to network security, although well known, are foregone.[15] New technologies that would create a more robust security network are, to the lament of many, under-developed. Rather than a distributed security dynamic, the current system is an assembly of off-the-shelf components in practice to maximize existing capacity.[16] Hence, partly because of over-dependence in market forces, the current system is left open and dangerously at risk. This benign neglect could, at some future point, be a root cause of a national catastrophe. Writing in 2006, Dan Verton remarked in *Black Ice: The Invisible Threat of Cyber Terrorism*:

> … the concept of allowing market forces to dictate security requirements remains the centerpiece of the [G.W. Bush] administration's policy on cybersecurity… government regulation of the Internet and software security requirements is out of the question.[17]

The author presses the point to suggest that such approaches to national security by the previous administration nearly abdicates any role it had for this

[12] Cyberspace Policy Review: Assuring and Trusted and Resilient Information and Communication Infrastructure, April 2009
[13] "Securing Cyberspace for the 44th Presidency," Center for Strategic and International Studies Commission Report, Washington, December 2008, p. 58
[14] Nasheri, Hedieh, p. 51
[15] Making the Nation Safer, p.145
[16] Ibid, p.141, 152
[17] Verton, Dan, Black Ice: The Invisible threat to Cyber-Terrorism, McGraw-Hill, Emeryville, CA 2006, p.25

responsibility.[18] The continuing competitive pressure of the free market economy has forced the world systems of communication and transport to outgrow the apparatus of international laws, codes, and commercial best practices standards. These factors facilitated trade in the industrial age. However, in the information age, the clash of modern technology, economic imperative, and the current structure of interstate relations is a significant hindrance to reform. Despite the complexity of the threat and the problems that a vulnerable ICT infrastructure present, a security regime at any level will not have consensus support if, at the same time, it does not enable business. The policy dilemma is how to assure that information is secure and commerce is not compromised. Cyberspace today, as with the global supply chain, bears a set of formidable traits: enormity of size, opaqueness, complexity, and hence - vulnerability. It is another anarchic realm where states sometimes view cooperation as contrary to national interest. Global corporations can simultaneously be victims and unsuspecting abettors of crime. It is also an environment where the definition of what constitutes illegal activity, acts of war, and ownership of property rights and accountability remain obscure. Furthermore, in addition to these conditions is the complexity of a struggle with "intimate and unavoidable" adversaries noted in the CSIS's report. Adversaries in this case can be state and non-state actors, previous foes or traditional allies. The world has changed dramatically since the inception of the Internet with the advancements in technology. The upgrade in architecture, security, and policy should also reflect the change in culture and the new nature of competition.

The Militarization of Cyber Space

From its beginnings as a closed military project cyber space has undergone several generations of evolution. With the commercialization of the Internet in the early 1990s, the increase in efficiency, reduction of cost, ease of access, and inherent insecurity has shaped the way we must now approach our method of interaction and commerce and the attendant issues of national defense and global competition. Today, it seems ironic that as the Internet expands to become a vast public good that we may be faced with the prospect of its re-militarization. However, in this scenario the reality is far more threatening and the consequences far less fathomable. As national borders become blurred by the imperatives of global commerce and manipulated by the lure of transnational crime, so do the roles of state and non-state actors become complex and transformative. The transformation may well determine the way we assess power alignments, rules of governance, and the separation of human, sovereign, and individual rights of privacy.

Despite the hope that many had that the information age would bring with it new accesses to empowerment and a spirit of democracy, the trend is that these hopes may give way to a revived and ominous era of competition between states. Signaling these developments, in November 2008, the U.S.-China Economic and Security Review Commission made the following recommendation to Congress:

> The Commission recommends that Congress urge the Administration to engage in consultations with its allies on an alliance based approach to dealing with cyber attacks originating in China.[19]

The study further asserts that Chinese military planners believe the United States is waging a cyber-based war on their nation, and therefore, in order to protect their intelligence and infrastructure assets China must develop its own capabilities. These "capabilities" will not only allow China to defend its own exploitable weakness, but also wreck havoc upon the U.S. system, which they believe is extremely vulnerable because of its dependency on information technology. Additionally, the authors maintain that part of China's strategy is the contention that pre-emption is key to the success in an outbreak of hostilities, either, conventionally or with respect to cyber operations.[20] However, in a report compiled by Chatham House, the assessment is that China's primary focus has been in preparation for counter strike capabilities, rather than a first strike maneuver. Yet, the same report goes on to say:

> In order to offset its conventional weakness the PRC is transforming its armed forces from a mechanized to an "information" force and have stated they intend to use information "as a tool of war or as a way to achieve victory without war."[21]

In the post-Cold War era of conflict cyber capabilities are asymmetric capabilities that allow a less armed opponent to engage a stronger military foe effectively and successfully. The ability to disrupt, delay, or obfuscate conventional operations affords those with limited military power a menacing defensive and offensive advantage. Without the release of a single missile, bomb, or lose of life, the United States could be completely paralyzed. Our dependence on inter-locking networks for commerce, financial services, communications, utility grids, government and military logistical needs, leaves the U.S. a nation at risk. Whether they are private sector networks, unclassified government archives, or classified and secure systems – all are vulnerable to varying degrees. What is more, as the general interviewed in the 2008 CSIS report asserts: *the war has begun.*

Beginning in 2003, investigators believe that cyber attacks originating in China have systematically and routinely been launched against government targets in the U.S. This massive cyber-espionage operation, codename "Titan Rain," is the archetype of post-modern warfare. The operation illustrates not only the paradigm shift of technology and strategy, but also the potential

[18] Yannakogeorgos, Panayotis, *Promises and Pitfalls of the National Strategy to Secure Cyberspace*, Division of Global Affairs, Rutgers University, 2009, p. 9-10

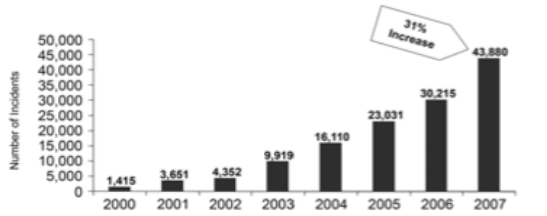
[19] 2008 Report to Congress of the U.S.-China Economic and Security Commission, p. 168

[20] Ibid. p. 166

[21] Cornish, Paul, Livingston, David, Clemente, Dave, Yorke, Claire, "On Cyber War," Chatham House Report, November 2010, p. 6

for power alignments and issues of governance for the extended future. More immediately, Operation Titan Rain reflects an inadequacy by our current defense structure to assess and respond effectively and even legally to such attacks. The assault calls into question issues over jurisdictional responsibilities, rights of privacy, and the roles of nation states and the private sector over accountability for security.

U.S. Department of Defense (DoD) Reported Incidents of Malicious Cyber Activity



Source: U.S.-China Economic and Security Review Commission, Hearing on China's Proliferation Practices, and the Development of its Cyber and Space Warfare Capabilities, testimony of Colonel Gary McAlum, Washington, DC, May 20, 2008.

According to a 2005 *Time* article, a mid-level systems analyst first uncovered Titan Rain while doing volunteer work for military intelligence.[22] Initially lauded by his government handlers for his work in discovering the intrusion, Sean Carpenter subsequently lost his security clearance and was fired from his job with Sandia Corporation. His offenses were the inappropriate use of company information and violating U.S. law by breaking into a foreign nation's computer system. Prior to his legal problems, Carpenter donated months of his time and energy to helping the Department of Defense and the FBI track down the source of these electronic intrusions. His investigation lead to the conclusion that information systems had been compromised from numerous U.S. Government agencies, including the United States Air Force, NASA, Redstone Arsenal military base, and also the World Bank. He believes the operations originated from Guangdong province in China and the information was warehoused somewhere in South Korea before finding its way back to Guangdong. Expert estimates claim that as much as 20 terabytes of information, or twice the print collection of the Library of Congress, was gathered.[23] Adding to his sense of betrayal by government authorities and company officials, Carpenter was dismayed that the investigative tools he acquired are not being used. After months of work he angers at the thought that no one: "…asked for the passwords or other tools that could enable them to pick up the investigative trail at the Guangdong router."[24]

According to the 2008 Commission Report to Congress, there may be as many as 250 hacker groups operating in China with either government support or "encouragement."[25] These individuals are often trained at Chinese military academies in cyber operations and the transference of such skills to the new arena of cyber war is seamless. As Robert Keohane and Joseph Nye have noted above, the environment of competition wrought by globalization has transformed and redefined military tactics. In their assessment it is not, necessarily, by design that "the asymmetry of global military power and the inter-connections among networks [has raised] new options for warfare." Yet, neither is it by mere random choice that they cite the Chinese in their examples as major players in the information war. The distrust from past conflict still lingers in the post-Cold War era of competition. Exacerbated by previous rivalries, today's thickening arena of increasingly, intensive and extensive web of international relations makes the combination of terrorism, drug trafficking, environmental degradation, and computer virus propagation attractive as well as cost effective and militarily potent.

In a conflict of such asymmetric weaponry the advantages of a cyber-strike are multiple and varied. Firstly, they can be launched instantaneously. A target would have little or no timeframe to prepare in defending itself. A second feature of an attack is the inability to establish attribution. Attribution, or the identification of the source of a cyber attack, is an issue of serious concern. Cyber attacks not only move at the speed of light, they occur in layers and travel along tortuously, indirect paths toward their objective. Since the current communication protocols lack the sophistication of the evolving array of hacking tools, it has become an increasing struggle for legitimate users to attribute incursions to a guilty source or point of origination. Therefore, by their nature, cyber attacks make it difficult for their victims to identify the enemy and, hence, retaliate appropriately. Finally, despite the absence of violence, cyber war can have the same destructive power as conventional warfare. Physical force, or a kinetic attack, aims to destroy an enemy's ability to wage war. Disabling a power grid, food supply, or any combination of elements of critical infrastructure can net the same result. Gen. James Cartwright, Vice Chairman of the Joint Chiefs of Staff claims that the consequences of a cyber attack could: "…be in the magnitude of a weapon of mass destruction."[26] Yet, these acts of aggression are without a multilateral consensus on whether they legally constitute acts of war.[27] The problem inhibits our ability to respond, re-organize our defense community, set standards, design and coordinate effective global cybersecurity policy, or fairly judge and discharge Sean Carpenter of his circumstances.

This asymmetric feature of cyber war is its most compelling for the United States. The strategic advantages once held by hegemonic powers in the interstate system are neutralized in the information age. The cost of "militarizing" cyberspace is low, and the

[22] Thornburgh, Nathan, *The Invasion of the Chinese Cyberspies*, "Time.Com," August 25, 2005
[23] Schifman, Jason, "The Need for a Strategic Approach to Cybersecurity," work in progress, University of Pennsylvania, April 2009, quoting Major General William Lord in "Air Force and the Cyberspace Mission Defending the Air Force's Computer Network in the Future," Center for Strategy and Technology, Dec 2007
[24] Thornburg
[25] 2008 Report to Congress of the U.S.-China Economic and Security Commission, p. 164
[26] Harris
[27] op. cit.

material resources are widely available. Therefore, the price of entry for less developed states and violent non-state actors is no longer an obstacle. Consequences of this paradigm shift in warfare are the proliferation of cyber warfare programs and development of non-traditional alliances between state and non-state actors, criminal gangs and terrorists organizations. [28] In this environment jurisdictional divides become meaningless to aggressors and create barriers for guardians of infrastructure assets and prosecutors of cyber crime. Furthermore, international codes of justice and best practices standards are unenforceable, and the attempts to establish order is uncoordinated and at times, insincere. As stated above, similar to the international supply chain, the system is plagued by its utter vastness and often, intended opaqueness. A colleague has described Cyberspace as: "an electromagnetic wilderness."[29] The authors of the CSIS report refers to it as:

> … part town square (where people engage in politics and speech), part Main Street (where people shop), part dark alleys (where crime occurs), part secret corridors (where spies engage in economic and military espionage), and part battlefield.[30]

Moreover, the technological threat vector posed by cyber war is metamorphic and tightly interlinked with the global economy. Adding to our dilemmas is the fact that the defense network in place to protect commerce and civil society is rooted in an interstate system encumbered by layers of formal protocol. Claims of national interest, state sovereignty rights, and political parochialism are the conditions of a former epoch and the mortmain, which hangs malignantly over the effort to adapt and meet the challenges of the new reality. Therefore, the conquest of this "wilderness" will require reorganizing society through policies that are more multilateral and, which can offer incentive for collaboration on a much grander scale. Otherwise, the alternative may be a partial return to Cold War power alignments and struggles with the addition of a cast of actors that include corrupt regimes, technologically sophisticated terrorists, and criminal organizations.

A Return to the Cold War

In the case of China, many analysts fear its leaders not only view cyber warfare as central to the overhaul of the national military, but also an important pathway toward economic development.[31] Aware of their comparative economic and military inferiority verses the U.S. the People's Republic of China (PRC) seeks to neutralize their disadvantages. By maximizing new realisms posited by the asymmetric environment of the information age, China hopes it can level the playing field.[32] A coeval of information technology has been the Revolution in Military Affairs (RMA). RMA is the application of IT to military purposes. The ever-expanding application of ICT and the rise of duel use technology have created a mesh of opportunities and risks ripe for exploitation. Since the end of the Cold War there has been a feverish effort by the American military to adapt its forces to the emerging paradigm. The effort has also been met by less powerful states and non-state actors, which recognize the relative competitive gains they can achieve militarily against traditional superior powers.[33] As expressed by the Chinese word for crisis, the confluence of these trends has offered up a convergence of opportunity and danger for China and its perceived rivals. It is a crisis that the PRC hopes to exploit against its adversaries on the one hand, and on the other hand, deflect as it seeks to defend its national interests.

According to Michael Pillsbury of the National Institute of Strategic Studies, China's own efforts to compete in RMA has resulted in projects known as *shashoujian* (assassin's mace). Having the project code number 998, *shashoujian* is believed to be a response to America's continued efforts in RMA and an important instrument in countering US hegemony in regional and global affairs.[34] Metaphorically, the term broadly refers to any action, technique, configuration of power, or technology deployed to overcome and reverse the tide of battle. The concept has been part of the discourse on military policy in China's since, at least, 2000.[35] In 1999 PRC President Jiang Zemin, a former Chairman of the Central Military Commission, declared:

> We should set great store by stepping up high technology innovation for national defense purposes and by developing technology useable for both military and civil purposes as well, and we should also master several *shashoujian* for safeguarding our national sovereignty and security as soon as possible.[36]

Compensating for its relative late arrival to cyber warfare, China attempts to gain parity with the US and Russia through projects such as *shashoujian*. For many in the military establishment, the inspiration for these efforts has origins in a Chinese proverb: "kill with a borrowed sword." The expression bespeaks of China's military policies that seek to overcome technological deficiencies with superior strategies.[37] "If you are limited in your strength, then borrow the strength of your enemy," so said Sun Zi, the legendary 2nd Century

[28] Yannakogeorgos, Panayotis, *Technologies of Militarization and Security in Cyberspace*, p. 14
[29] Ibid, p. 1
[30] "Securing Cyberspace for the 44th Presidency," Center for Strategic and International Studies Commission Report, Washington, December 2008
[31] Schifman, p. 12-14
[32] Johnston, Alaster Iain, "Toward Contextualizing the Concept of a *Shashoujian* (Assassin's Mace), Harvard University Government Department, Aug. 2002, P. 27
[33] Kaldor, Mary, *Beyond Militarism, Arms Races, and Arms Control*, essay prepared for the Nobel Peace Prize Centennial Symposium, December 2001
[34] Ibid
[35] Pillsbury, Michael, *China's Military Strategy Toward the U.S.: A View from Open Sources*, US-China Economic and Security Review Commission, November 2001
[36] Johnston, p. 325
[37] Thomas, Timothy L., "China's Electronic Strategies," in *Military Review*, May-June 2001

BCE military strategist and traditionally recognized author of The Art of War. By taking the advice from an ancient text, China has girt itself to vigorously compete in the cyber conflict. As part of this strategy, the People's Liberation Army (PLA) has been establishing and cultivating relationships with patriotic hackers. "Hacktivism," or the combination of political activism and computer hacking, has evolved into a new phenomenon – state hacktivism. State hacktivism involves patriotic hackers who are motivated for nationalistic reasons, and operate in the service of their countries. In this practice area, China is particularly expert in organization and recruitment. The government sponsored Network Crack Program Hacker (NCPH), identifies proficient groups of hackers through competitions. Those selected receive monthly stipends from the PLA. According to Panayotis Yannakogeorgos of Rutgers University, they are recruited to not only ply their craft on foreign targets, but also to teach army cadets the tactics and tools for conducting cyber war. Joel Brenner, a former senior government counterintelligence official whose past posts include inspector general for the National Security Agency and chief executive of the Office of the Directorate of National Intelligence remarks about China's cyber-threat:

> Some [attacks], we have high confidence, are coming from government-sponsored sites. The Chinese operate both through government agencies, as we do, but they also operate through sponsoring other organizations that are engaging in this kind of international hacking, whether or not under specific direction. It's a kind of cyber-militia …It's coming in volumes that are just staggering."[38]

Not only as political rivals, but also as business partners, China has capitalized on the "borrowed sword" to breach security defenses and make gains in the struggle over cyber space. American and non-U.S. based ICT firms are often unwitting hosts of the strategy.[39] Competitive pressures force U.S. companies to rely on China's outsourced production facilities to assemble and manufacture products. Because of the efficiencies of the extended enterprise, the attractive pricing of products from developing countries and transition economies, and the dynamic of the global market place, Western companies are irresistibly lured into commercial alliances with non-Western partners. These joint venture arrangements are openings for a hostile player to implant viruses, malware, Trojan horses, and backdoors into equipment for proprietary civilian and military use. Once commercially available, the corrupted technology and component parts can infest systems anywhere in the world. The subversion of information systems is subtle, mostly impossible to detect, and potentially ruinous. The disabling of the U.S. Pacific Command Headquarters has been attributed to the use of malicious code produced in China.[40] According to some reports, a State Department official released a Trojan horse by opening an e-mail. This allowed a hacker covert access and denied PAC Command Internet use.

Through these same methods, Chinese hackers have also been credited with electronic intrusions against the State Department, the Department of Defense, Energy, Agriculture, Treasury, and Health and Human Services. For obvious reasons, the Pentagon and its sprawl of private contractors are particularly targeted. Boeing, Raytheon, General Dynamics, General Electric, and Lockheed Martin have all experienced attacks from cyber spies looking for sensitive information.[*]

Source codes, or the software programming instructions, are particularly appealing targets. The ability to copy or corrupt these millions of lines of instruction gives hackers the capability of tunneling into information systems around the world. Once the information is accessed, there is little to prevent someone from stealing intellectual property and inserting their own code. According to Google, this is precisely what has occurred not only to them, but at least 30 other California-based companies.[41] In addition, over the past several years, counterfeit Cisco routers have surfaced. Their intrusion creates the fear that implanted software could give foreign or other unauthorized agents the capability to tap into networks with the same ease as law enforcement agencies.[42] As required of network hardware manufacturers by law, Cisco Systems produces according to specifications that allow the U.S. government wire-tapping capability for investigative purposes. In such a case, a corrupted router: "could provide the perfect over-the-shoulder view of everything coming out of a network" according to Jeff Moss, a security expert with the Homeland Security Advisory Council.[43]

From a military standpoint, these capabilities can expose a nation to a new scope and dimension of threat. Quoting the commander of the Air Force Cyber Command: "You don't need an army, a navy, an Air Force to beat the U.S., you can be a peer force for the price of the PC on my desk."[44] What can, and perhaps has resulted is an "Internet too unwieldy to be tamed."[45] What may have also been unleashed is "espionage on a massive scale," says Paul Kurtz of the security consulting firm, Good Harbor Partners.[46] In support of these

[38] Harris
[39] Yannakogeorgos, *Technologies of Militarization and Security in Cyberspace*, p. 72-3
[40] Barret, Barrington M., "Information Warfare: China's response to U.S. Technological Advantages," *International Journal of Intelligence and CounterIntelligence*, 18 No 4, 2005
[*] These threats not only originate from China. The rise of new centers of design and production across the globe has created new opportunities for hardware and software manipulations by state and non-state actors.
[41] Markoff, John, Vance Ashlee, "Fearing Hackers Who Leave No Trace," *New York Times*, January 20, 2010
[42] Ibid
[43] Ibid
[44] Lord, William T., in "The New E-spionage Threat," *Businessweek*, April 2008
[45] Grow, Brian, Epstein, Keith, Tschang, Chi-Chu, "The New E-spionage Threat," *Businessweek*, April 2008
[46] Ibid

statements, current estimates claim Department of Defense computers undergo millions of scans on a daily basis along with thousands of potentially damaging probes.[47]

Although China is often cited as the greatest cyber menace to the U.S., Russia's military programs and adventures in cyberspace may have been the most conspicuous. The end of the Cold War, the restructuring of power alignments, and the passing of U.S.S.R. has not dismantled Russia's technological/industrial base or diminished its capability. The Russian assault on Estonia's e-government operations and electronic incursions into Georgia was early evidence of Russia's prowess and intent. It was also indication that the cyber world was becoming militarized and the fears of military experts were, perhaps, well founded.

During protests and retaliation for the removal of a statue at a Soviet era war memorial in Tallinn in 2007, not only were Estonian government ministry websites taken out, but those of political parties, news agencies, banks, and telecommunication companies also disabled.[48] Gen. William Lord is Chief of Warfighting Integration and Chief Information Officer for the Air Force. A minister of defense in this nation of 1.3 million reportedly admitted to him that "one million computers" attacked his country.[49] The electronic offensive by Russia raised alarms and cut at the core of the NATO alliance. Cries of concern about issues of collective self-defense rose to the surface and almost as quickly became muted because of a lack of definition, precedent, framework for resolution, and any clear policy guidance on an appropriate response. At the time there were also bitter disputes between Russia and former Soviet republics and Eastern satellite states. This electronic incursion may have been an act of frustration, or a signal to its rivals that Russia was prepared to open a new field of conflict to press its grievances. Prospects for how policy could be set to attend to future state sponsored incursions were faint, if not dark. As officials struggled to make public statements and offer assurances that the situation would be seriously addressed, the system of state relations was experiencing a new strain of "machtpolitik" that, in effect, stifled these policymakers and frustrated their efforts to act.

The year following the strike on Estonia, Russia combined military operations with a cyber attack against the Georgian government. Through a cyber-criminal organization known as the Russian Business Network, an electronic assault on government websites crippled Georgia's public information infrastructure.[50] Unlike the Estonian event, these attacks were coordinated with an armed invasion force. However, it was not the first time Russia employed cyber technology alongside military action. In 2002 a similarly orchestrated attack of armed kinetic force and an electronic incursion against servers occurred in Chechnya. As in the case of China, the Russian government has officially disavowed connection with any cyber offensive by itself or others working on its behalf.

Because of the U.S.'s lead in the information war, Russia's anxiety over the competition in cyber space arouses the same tensions, as had the Cold War period. The technology gap, national paranoia, recurring xenophobia, and a history of distrust have helped shape an emerging Russian worldview with roots in an old fortress state mindset. Foreign affairs correspondent, James Adams, writes:

> [Russian military officials] want to transmit a common message that Russia is a nation at war. It is an information war that the country is losing at home and abroad, and the current technology gap is comparable to the perceived missile gap of the 1950's that did so much to fuel the Cold War. This time, the race is not for space, but cyber space. And all the Russians are angry that America appears to be winning the war and that victory appears more assured every day.[51]

Therefore, Russia is considering building its own Internet in order to de-link from the present system. The Internet, which the United States designed, developed, and now controls 80% of the infrastructure, has become a security risk for Russia's national defense and strategic interests. Efforts at international conferences and summits to establish accords and norms for the regulation of cyber space have become tug-of-wars between the United States and Russia. Under dispute are not only the language of laws, but also the fundamental nature of their purpose. The U.S., naturally, opposes restrictions in a sphere of activity where it holds a compelling advantage. On the other hand, under-advantaged states push for a more regulated environment in order to lessen their vulnerability and exposure to cyber risks. In much the same way local industry might seek economic protection from its government against foreign competition with competitive advantages; Russia pushes hard in these negotiations for regulatory control. This tactic is usually regarded by the U.S. as an attempted "protectionist policy" that allows Russia to buy time while it works to narrow the technology gap and level the playing field.[52]

Some analysts believe, however, that this kind of shortsightedness by the United States may lead to an Information Age weapons race.[53] Other experts have already warned; "major governments are reaching the point of no return in heading off a cyber-war arms

[47] Lynn, William, Deputy Secretary of Defense, in "US Creates Military Cyber Command to Defend Computer Networks," *Global Security*, 15 June 2009

[48] "Russia Accused of Unleashing Cyberwar to Disable Estonia," *Guardian*, May 17, 2007

[49] Harris

[50] "Georgia's State Computers Hit by Cyber Attack," *The Wall Street Journal*, August 12, 2008

[51] Adams, James, "The New Arms Race," in the Next War: Computers are the Weapons and the Frontline is Everywhere," Hutchenson, 1998 in Yannakogeorgos *Technologies of Militarization and Security in Cyberspace*, 72-3

[52] Adams in Yannakogeorgos

[53] Thomas, Timothy, "Russian View of Information Based Warfare, *Airpower Journal*, 1996, in Yannakogeorgos, *Technologies of Militarization and Security in Cyberspace*, p. 72-73

race."[54] Such weapons in this conflict include the following:

- **Logic bombs**, which can be spawned by a Trojan horse. Once embedded within a system can damage circuitry or cripple operations at critical points and times. These are internal bits of code programmed to activate upon a certain condition, event, date, or time.
- **Botnets** are an array of computers, which run applications controlled by their owners that spy and disable networks and websites.
- **Trapdoors** bypass the security of programs under development. The developer's intension is to create a "hole" in the security framework of the program for exploitation at a future time. Only the creator of the trapdoor is aware of its existence once the program is in operation.
- **Bacteria** replicate itself and damages device storage resources by overloading disks and memory capacity.
- **Viruses**, unlike bacteria, carry malicious code. They can only attack programs or data in order to replicate themselves. Viruses pass through dormant and triggering phases before performing its function, in which results range from benign defacement to total system ruin.
- **Microwave** radiation devices burn out computer circuits from miles away.

In this intensifying high stakes game, there is also the belief that Russia is secretly enlisting China in support of its efforts to shape international policy on arms control treaties in cyberspace.[55] Whichever side prevails, the possibility to wreck havoc and plunge the world into a new epoch of confrontation is not only real, but already upon us.

However, December 2009 may signal a turning point in negotiations over the militarization of cyberspace. During this period, talks began between the U.S. and Russia regarding the possibility of international treaties to address the challenges posed by cyber warfare. Despite many contentious items, a common ground may be in the United States' interest to control Internet crime versus Russia's apprehension over cyber weapons development and proliferation.[56]

The parallels to the old order appear striking. Yet, at the same time, the configuration of power alliances would be a stark break with the past. According to a 2009 report commissioned by McAfee, Inc., criminal organizations are becoming more motivated by nationalistic pride rather than mere monetary gain. A prime example is Russia. The authors of the report cite McAfee's own Vice President of Threat Research, Dmitri Alperovitch who maintains that a righteous attitude toward the West is propelling much cyber crime. An indication of these moral postures is found in a warning posted on an online forum:

> We will recreate historical fairness. We will bring the USA down to a level of 1928-33.[57]

Spheres of influence would not be geopolitical but "virtual-political." Rather than bound by territorial jurisdictions and state borders, hegemons and their satellites would be linked by electronic connections. Whether associated by cultural and traditional ties, or motivated by unadorned, economic self-interest, the new order would be a constellation of states, corporations, terrorists, criminals, and social activists. Within this arrangement, it would be difficult for any single participant to have a monopoly on violence or arms control. Determining the extent and impact of the anarchy is impossible to suppose.

Net War and Net Warriors

Cyber space infrastructure is the critical underpinning of the global economy and, therefore, its integrity is essential to national security, public safety, and modern civic intercourse. The hyper-interconnection, which evolved parallel with globalization expanded opportunities for all. Whether those opportunities are used as a way for people to improve their lot, or destroy the quality of life of others is beyond its original design and control.

The asymmetry of today's warfare and the accessibility, anonymity, and ubiquity of the Internet has created opportunities for transnational crime organizations and international terrorism to plunder and recruit. Like state sponsored programs, these non-state actors have the capability to disrupt utility grids, telecommunications networks, defraud businesses and financial institutions, and disable and compromise government sites. Examples include:

- In 1995 the successful intrusion into U.S. Government files and downloading of sensitive information concerning North Korea's ballistic weapons research. The culprit was a sixteen-year-old British student[58]
- 1999 – the "Melissa" computer virus, which caused over $80 million in damages to personal computers, business and government networks by infecting e-mail gateways and clogging systems[59]
- An attempt to divert $400 million of EU funds from regional development projects in 2000. The funds were to be laundered through various online components of major money center banks, including the Vatican bank. Interdiction

[54] Ibid
[55] Markoff, John, Kramer, Andrew E., "U.S. and Russia Differ on Treaty for Cyberspace," *New York Times*, June 28, 2009
[56] Markoff, John and Kramer, Andrew, "In Shift, U.S. Talks to Russia on Internet Security," *New York Times*, December 132009
[57] "Virtual Criminality Report 2009,"Commissioned by McAfee, Inc., prepared by Paul Kurtz, Good Harbor Consulting, 2009, p. 12
[58] Schifman, p. 2
[59] Nasheri, p. 104

occurred only due to the misgivings of a co-conspirer who eventually, turned informant.[60]

- The financial support of the 2002 bombings in Bali, which police claim were provided by funds obtained through online credit card fraud[61]
- A Russian based hacking operation, which involved fraud and extortion in 2003. Aggregate losses amounted to approximately $25 million.[62]
- The 2004 investigation and termination of a criminal organization that involved 4,000 members engaged in stolen identities and credit card information. Known as "Operation Firewall," this Secret Service exercise culminated in the elimination of a major hub for online identity theft [63]
- The 2005 conviction of a Massachusetts juvenile responsible for the theft of personal information and initiating panic with bomb threats. The convicted hacked into Internet and telephone service providers over a 15-month period before being apprehended.[64]
- On May 2006, the Department of State believed its networks were hacked by unknown foreign intruders resulting in the download of terabytes of information.[65]
- May 2006, a public statement by a senior Air Force Officer reveals that "China has downloaded 10 to 20 terabytes of data from NIPRNet"[66]
- NASA blocks email prior to shuttle launches fearing harmful attachments in December 2006. At the same time Business Week reported that unknown foreign agents had obtained the plans for the latest space launch vehicles.[67]
- The Bureau of Industrial Security, which reviews high tech exports at the Department of Commerce, had its networks hacked by foreign intruders and forced off line for several months in April 2007.[68]
- In May 2007 "the National Defense University had to take its email systems offline because of hacks by unknown foreign intruders that let spyware into the system."[69]
- Reportedly, in August 2007 the British Security Service, the French Prime Minister's Office, and the Office of German Chancellor Merkel complained to the PRC about electronic intrusions.[70]
- A compromise of a major U.S. retailer's database that resulted in the loss of information of 45 million credit and debit card accounts in 2007[71]
- Databases of the Republican and Democratic presidential campaigns were hacked into by unknown foreign sources over the summer of 2008[72]
- In November 2008 classified networks at the DoD and CENTCOM were hacked and disabled for several days before the systems could be restored[73]
- The corruption of 130 ATM machines that produced fraudulent transactions in 40 cities in 2008[74]
- The estimated losses of $1 trillion due to intellectual property theft in 2008 [75]
- January 2009 – Israeli's internet infrastructure was paralyzed during that country's military offensive in the Gaza Strip. The attack, which concentrated on government websites, was launched from within the former Soviet Union and financially supported by Hamas or Hezbollah officials believe.[76]
- February 2009 –French combat aircraft were grounded following the infection of databases by a computer virus known as "conflicter."[77]
- March 2009 – Canadian researchers uncover a computer espionage system implanted in government networks of 103 nations. The researchers attribute the effort to China.[78]
- March 2009 – on a file sharing network in Iran, the plans for the new presidential helicopter, Marine 1, are discovered.[79]
- May 2009 – Unknown hackers gain access to the data in the Homeland Security Information Network (HSIN) collecting data on federal, state, and local employees and contractors.[80]
- June 2009 – the Applied Physics Laboratory of John Hopkins University had its networks penetrated and eventually forced to go offline.[81]
- June 2009 – Wolfgang Schaeuble, German Interior Minister, noted in a security report that

[60] Williams, Phil, "Organized Crime and Cybercrime, Synergies, Trends, and Responses," in Global Issues 2001, US Information Agency
[61] Cybercrime – Public and Private entities Face Challenges in Addressing Cyber Threats, GAO Report to Congressional Requesters, June 2007, GAO-07-705
[62] Ibid
[63] Ibid
[64] Ibid
[65] Lewis, James, "List of Significant Cyber Incidents Since 2006," Center for Strategic and International Studies, http://csis.org/publication/23-cyber-events-2006, posted June 12, 2009
[66] Ibid
[67] Ibid
[68] Ibid
[69] Ibid
[70] Lewis, James, "List of Significant Cyber Incidents Since 2006," Center for Strategic and International Studies, http://csis.org/publication/23-cyber-events-2006, posted June 12, 2009
[71] Cyberspace Policy Review: Assuring and Trusted and Resilient Information and Communication Infrastructure, April 2009
[72] Lewis, Op. Cit.
[73] Ibid
[74] Cyberspace Policy Review: Assuring and Trusted and Resilient Information and Communication Infrastructure, April 2009
[75] Cyberspace Policy Review
[76] Lewis, James, "List of Significant Cyber Incidents Since 2006," Center for Strategic and International Studies, http://csis.org/publication/23-cyber-events-2006, posted June 12, 2009
[77] Ibid
[78] Ibid
[79] Ibid
[80] Ibid
[81] Ibid

China and Russia have been increasing espionage efforts and cyber attacks on German firms.[82]

- Critical infrastructure attacks on targets in the U.S. and overseas leading to outages at electrical power stations in multiple locations and cities[83]
- The FBI claim that Al Qaeda terrorist cells rely on stolen credit card information as financial support. [84]
- The CIA identification of, at least, two known terrorist organizations with the capability and intent to launch cyber attacks on the U.S. infrastructure [85]
- Due to cyber attacks, an estimated annual direct loss of $67.2 billion for U.S. organizations according to 2005 figures [86] and a revised figure of over $1 trillion worldwide for 2008[87]

Despite the volume of evidence to support justification for alarm, data on these assaults do not reflect the true scale of the problem. Public records are not only inaccurate due to detection issues, but often times by sheer intent. Reports are obviously lacking when victims are unaware of electronic intrusions. Frequently, because of manpower and technical skills deficit, cyber-crime goes on unmasked and with no ill consequences for the perpetrator. However, when cyber crimes do surface there are incentives for the injured party to keep these accounts out of the public realm. The consequences for victimized organization can be dismaying. The fear of negative publicity is always a concern for private sector enterprises as well as public offices and organizations. In the case of a security breach of a business firm, the instance can open an organization to lawsuit and adverse market impact. Studies at Georgia Tech reveal that firms that experience an interruption of operations will suffer an attendant decline in stock value. Furthermore, depending upon the duration of downtime, recovery can extend over several business quarters. This is particularly true if it involves a financial institution.

Public disclosure of security failure can also be a signal to attackers that vulnerabilities exist and an organization may be ripe for exploitation. With these circumstances also come fears of job loss and the demise of reputations. In weighing the costs and impact of reporting such incidents, it is easy to understand why many organizations opt to remain silent about their situation rather than draw public attention. Additionally, the allocation of time and resources, as well as the poor record of prosecution create further disincentive to report such offenses. The era of cybercrime has created a new set of legal problems and issues. Theft infers possession, which is a difficult, delicate, and more complicated argument when the property is intellectual rather than tangible. Furthermore, the information disclosed during the process of cross-examination can run the risk of be as damaging to the plaintiff's self-interest as the original crime.

Regardless of the reticence to admit to these victimizations, the economic loss to business and the consumer is still staggering. According to the GAO 2007 report, the direct losses due to computer crime, without an estimation of related costs, are $67 billion. Identity theft via electronic means amounts to over $56 billion. Worldwide, over $100 billion in losses from spam annually occurs. Spamming is more than a simple nuisance. Not only a malicious way to clog a system, span can act as a carrier for malware and a host of other cyber threats.[88] Dan Dunkel, President of New Era Associates, a security consulting firm says:

> With tremendous technical advantages come potentially devastating risks. As digital citizens we lack a fundamental "open" dialogue to confront the obvious trends in international cyber crime, or to address the complex technical, business and legal issues that will ultimately better secure cyberspace. We need to make cyber crime and security an international priority.[89]

As stated above, these numbers not only reflect an unknown percentage of unreported and under-reported incidents, they also represent a statistic, which continues to rise. The cybersecurity threat is outpacing our our attempts at a solution. It hovers over us at the national, organizational, and individual level. The global economy, and perhaps, our way of life may be at risk. A Senior Advisor at the Belfer Center at the John F. Kennedy School of Government at Harvard, Melissa Hathaway writes:

> I believe that we are at a strategic inflection point – and we must band together to understand the situation and ascertain the full extent of the vulnerabilities and interdependencies of this information and communications infrastructure that we depend upon. As I reflect upon the situation, one of the key recurring questions is whether we really understand the intersections of our critical assets and the networks and how we as entities interface with the communications infrastructure and the energy grid and other critical services that are provided on the backbone of interdependent networks.[90]

Understanding the power and opportunity of cyberspace infrastructure is not complete without an understanding its fragility and our vulnerability should it fail. The table

[82] Lewis, James, "List of Significant Cyber Incidents Since 2006," Center for Strategic and International Studies, http://csis.org/publication/23-cyber-events-2006, posted June 12, 2009
[83] Cyberspace Policy Review
[84] GAO Report to Congressional Requesters, June 2007, GAO-07-705
[85] Ibid
[86] Ibid
[87] Hathaway, Melissa, *Five Myths About Cybersecurity,* Belfer Center for Science and International Affairs, John F. Kennedy School of Government, December, 21, 2009
[88] GAO Report to Congressional Requesters, June 2007, GAO-07-705
[89] Dunkel, Dan, President, New Era Associates, interview, December 2010
[90] Hathaway, Melissa, "Strategic Advantage: Why America should Care About Cybersecurity," Belfer Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University, October, 2009, p. 1

below represents the various technique categories of cybercrime and a brief description of their methods and harmful effects.

Table
Techniques Used to Commit Cybercrimes

Type	Description
Spamming	Sending unsolicited commercial e-mail advertising for products, services, and Web sites. Spam can also be used as a delivery mechanism for malware and other cyber threats.
Phishing	A high-tech scam that frequently uses spam or pop-up messages[a] to deceive people into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, or other sensitive information. Internet scammers use e-mail bait to "phish" for passwords and financial data from the sea of Internet users.
Spoofing	Creating a fraudulent Web site to mimic an actual, well-known Web site run by another party. E-mail spoofing occurs when the sender address and other parts of an e-mail header are altered to appear as though the e-mail originated from a different source. Spoofing hides the origin of an e-mail message.
Pharming	A method used by phishers to deceive users into believing that they are communicating with a legitimate Web site. Pharming uses a variety of technical methods to redirect a user to a fraudulent or spoofed Web site when the user types in a legitimate Web address. For example, one pharming technique is to redirect users —without their knowledge—to a different Web site from the one they intended to access. Also, software vulnerabilities may be exploited or malware employed to redirect the user to a fraudulent Web site when the user types in a legitimate address.
Denial-of-service attack	An attack in which one user takes up so much of a shared resource that none of the resource is left for other users. Denial-of-service attacks compromise the availability of the resource.
Distributed denial-of-service	A variant of the denial-of-service attack that uses a coordinated attack from a distributed system of computers rather than from a single source. It often makes use of worms to spread to multiple computers that can then attack the target.
Viruses	A program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. A virus requires human involvement (usually unwitting) to propagate.

Vulnerabilities

Perhaps one of the primary roots of our vulnerability is SCADA, supervisory control and data acquisition system. SCADA systems are computer systems, which automate, monitor, moderate, and control industrial plant functions and critical infrastructure. The technology is ubiquitous. The power grid is particularly dependent upon SCADA. As with the original Internet, these systems were designed with little attention to security. Data is sent "in the clear," or over open pathways that rely on the Internet and often require no authentication.[91] Furthermore, for economic reasons and owing to an enduring spirit and environment of deregulation, SCADA systems increasingly depend upon commercial off-the-shelf (COTS) components as security patches and to optimize existing capacity.[92] [93]

The use of COTS as security countermeasures may not only be perilous, but also impractical according to at least one independent analysis. A study by the University of California, Berkeley and Carnegie Mellon University asserts that patching and frequent updates may be unfeasible for control systems in certain instances. Upgrades sometime take months of advance planning and require suspension of operations. Therefore, the justification for installing security patches may be negated by economic considerations or market demands. These patch updates may also violate manufacturer certification under certain conditions and open the operator up to litigation.[94] These concerns, combination of control systems' vital role in critical infrastructure operations, and the general awareness of the lack of security used in their design and support, make SCADA systems attractive targets for malicious hackers, criminals, or terrorist agents.

Additionally, SCADA not only manages the soft elements of the network, which are associated with disruption issues, but physical elements fall under these systems' controls as well. Therefore, physical damage may result in the destruction of infrastructure. The long-term consequences are networks, which have to be rebuilt, and their components must be remanufactured from scratch.[95] The fragility of the entire system is further compounded by the ironies of an open Internet. According to the National Research Council's Committee on Science and Technology for Countering Terrorism, these vulnerabilities are widely known and details on our

[91] National Research Council of the National Academies, Making the Nation Safer: The Role of Science and Technology in Countering Terrorism, The Committee on Science and Technology for Countering Terrorism, The National Academies Press, Washington, DC 2002, p. 140-141
[92] Ibid
[93] Schifman

[94] Cardenas, Alvaro A. Amin Saurabh, Sinpoli, Bruno, Giani, Annarita, Perrig, Adrian, Sastry, Shankar, "Challenges for Securing Cyber Physical Systems," Report prepared by the Department of Electrical Engineering and computer Sciences, University of California, Berkeley, Department of Civil and Environmental engineering, University of California, Berkeley, and the Department of electrical and Computer Engineering, Carnegie Mellon University with a grant from the National Science Foundation
[95] National Research Council of the National Academies, p. 140

exposure are accessible to all on the World Wide Web. In the committee's 2002 report, it states:

> Product data and educational video tapes from engineering associations can be used to familiarize potential attacker with the basics of the grid and specific elements. Information obtained through semi-automated reconnaissance to probe and scan the networks of a variety of power suppliers could provide terrorists with detailed information about the internals of the SCADA network, down to the level of specific makes and models of equipment used and version releases of corresponding software. And more inside information could be obtained from sympathetic engineers and operators.[96]

Stephen Flynn, in his 2007 book, The Edge of Disaster, reveals in one example how precariously tethered national security is to the national power grid. He cites a 2006 report by Siobhan Gorman of the Baltimore *Sun*. In the report the NSA feared the installation of two supercomputers would overload an already extended power grid. Under such stressed conditions the agency concluded that the longest period of time the electrical infrastructure could forestall a collapse of the system was two years. In the event of a meltdown, it would take between 18 to 30 months to design and procure equipment, obtain permits and build a new power station. In the interim, the NSA's ability to process its work and operate normally would be severely hampered.[97]

The U.S. electrical power grid, according to Gilbert Bindewald of the Department of Energy's Office of Electricity Delivery and Energy Reliability: "was never holistically designed," and "developed incrementally in response to local load growth."[98] The result is a service environment of constant change and uncertainty. The system's complexity, decentralized flow control, and fluctuating dynamic of consumer usage contribute additional challenges to security. A sudden drop in voltage, either because of uncontrolled demand or the result of false information inserted into SCADA could cause collapse.

There are many examples where the manipulation of the computer code could have devastating effect on critical infrastructure. According to Bindewald: "electricity [is] the ultimate just-in-time production process".[99] The absence of flow control, and the lack of any large-scale storage capacity make the electric power grid unique and vulnerable. The same features that propel and permeate our commercial way of life are the symptoms of our deficient immunity to a cyber attack.

Today the power grid is decentralized, aging, susceptible to blackouts, reliant on SCADA, and under increasing demand due to the expanding digital economy.[100] Only by making the grid "smarter" or by changing the supply mix (using alternative energy sources) can the power infrastructure and our daily routines be made more secure. However, these are mostly longer-term solutions, and the vulnerabilities we face represent prevailing conditions.

Already, there have been several reports involving major power outages by Internet enabled intrusions.[1179101] Some relate to instances abroad. However, the August 15, 2003 power black outs, which occurred in the northeast U.S., have opened up a discussion about the grid's vulnerability to hacker activity. In the intelligence community, speculation persists that the outage can be attributed to China or agents working in collaboration with the PLA. The 2003 outage affected 50 million people in three states, including Canada. It covered a 9,300 square-mile area and had an estimated economic toll of between 6-10 billion dollars.[102] The cause of the power failure has, arguably, never been fully understood. However, many of those in the counterintelligence community believe the PLA gained access to one of the networks that controlled electric power systems. The result was the greatest blackout in North American history.[103]

Officially, no involvement by a foreign government or national has been cited. Rather, "overgrown trees," which came into contact with high voltage lines are credited with the failure of more than 100 power plants in Michigan, Ohio, New York, and north of the border. A widespread computer virus supposedly put the system over the edge by disrupting the communication lines used to manage the power grid.[104] Whether an ill-timed event or an event by design, the outage forced one industry analyst to assess "that security for the nation's electronic infrastructures remains intolerably weak" and to also emphasize that the incident confirms "government and company officials haven't sufficiently acknowledge these vulnerabilities."[105]

Another outage in 2008 also raised speculation of hacker intrusion originating from China. A power failure cut off 3 million customers of Florida Power & Light along the state's east coast. The company blamed "human error" for the disruption. However, there are some inside government and industry who maintain that hackers inside China, have devoted considerable resources to mapping and analyzing the U.S. critical infrastructure, and by mistake or with intension, may have set off the incident.

As discussed, the Chinese are not alone in their quest for advantage in cyberspace. In fact, it was also reported that computer intrusions penetrated European utilities in 2006, and that assaults similar to these might have a history as far back as the Cold War. According to a press report in 2004, a portion of the Siberian pipeline

[96] Ibid
[97] Flynn, Stephen, The Edge of Disaster, Random House, New York, 2006, p. 83.
[98] Bindewald, Gilbert, "Monitoring and Modeling of the Electric Power System," Presentation, October 28, 2009.
[99] Ibid
[100] Bindewald

[101] Hathaway, Melissa, "Strategic Advantage: Why America should Care About Cybersecurity," Belfer Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University, October, 2009, p. 13. Yannakogeorgos, Panayotis, *Promises and Pitfalls of the National Strategy to Secure Cyberspace*, Division of Global Affairs, Rutgers University, 2009, p. 22-23.
[102] Flynn, The Edge of Disaster, p. 69
[103] Harris
[104] Ibid
[105] Ibid

exploded in 1982 with the use of a logic bomb.[106] Today, the field is populated with many competitors and combatants. The warfare is asymmetrical, unpredictable, and absent of any conventional wisdom – yet, the questions are always the same: Who is the enemy? What are their intent and objectives? How do we maintain our security while enabling our work and protecting way of life?

In summary, cyberspace has become the new battlefield because it is the core of critical infrastructure and industrial control systems. Although this has been the situation for decades, attacks have been randomly confirmed, and many more have gone unreported or undetected. Sources of attacks are myriad. Cybercriminals, disgruntled employees, terrorists, activists, organized crime, and state actors all have their own resources and motivations. Meeting the challenges of these security threats is achieved through prevention, detection, recovery, resilience, and eventually-deterrence. However, the war is asymmetrical and, at present, the technological advantage is with the attacker. Offensive action is easier, cheaper, and quicker than it is for defensive action.[107] This is partly due to the fact the range of possible targets is almost endless. It is also due to the obsolescence of the overall infrastructure and an early insouciant attitude toward security. A third frustration is the fact that the action/reaction cycle to the threat is so sudden that the very innovation used to address the original vulnerability can create further instability.

Conclusion

In cyberspace we are hyper-connected to a series of networks where lines between private and public security blur. At the same time the linkage in human affairs is organic, as competitive and complementary impulses drive events while we all undertake to ply at our work and live our lives. In common is our need to conduct business, power our households, access financial assets, provide and receive healthcare. Therefore, the security of these networks is central to our way of life. The fragility of these networks and our reliance upon them puts us in a perilous state. We are vulnerable to a host of threats from state and non-state actors, natural disasters, and our own overuse of valuable resources.

Moreover, the transition from the industrial age to the information age has been disorienting for strategists and policy makers. The imperatives of international trade and commerce have suppressed the calls for investment in security. Economic policies, which require unquestioned faith in the market and posited the belief in privatization programs, while heaping scorn on government and regulatory involvement may have put the system on to a precarious ledge. What exists is a cybersecurity understructure resembling a Rube Goldfarb contraption of patches and workarounds unsuited to accommodate the traffic demands of SCADA systems and custom large-scale implementations. As Mark Cohn, a thought leader and Vice President of Enterprise Security at Unisys Corporation remarks:

> The marketplace driven interconnectedness that we have been so excited about over the last twenty years combined with orders of magnitude changes in available bandwidth put some of those systems in to a mode their designers never envisioned: we can't unravel those trends and backtrack but we did, in fact, know how to build fault tolerant systems that in some cases never failed and could apply the same engineering approaches for a "smart grid" if it were possible to arrange the right political and economic circumstances.[108]

The landscape of town squares, Main Streets, dark alleys, secret corridors, and open battlefields that the CSIS Commission Report described, is not a static environment. It is dynamic, and instability is an accepted condition – for now. Many fear that without an open debate, the condition will remain chronic. As the above metaphor infers, cyber conflict ensnarls many actors, on varying levels, and in so many ways. Furthermore, because the environment is so target rich, the establishment of order may require new partnerships between the public and its government, a rewriting of legal codes, and new mechanisms for mobilizing society.

In addition, a frighteningly, deadly backdrop to the above scenario is the prospects that as sub-state actors are becoming key players, an inter-state cyber Cold War may have already begun. Under the conditions of asymmetrical warfare, nation states and cyber criminal groups can make for natural allies. Cyber war and cybercrime employ the same weapons and require the same skills. However, the skills and weapons may now be for sale. We may be at the onset of an inter-state war among past Cold War rivals and, simultaneously, engaged in an asymmetric conflict of non-state players. A cyber expert claims:

> Many of the challenges of cyber war mirror those of in cybercrime because nation states and cyber gangs are all playing from the same instruments. For instance, anyone can go to a criminal gang and rent a botnet. We've reached a point where you only need money to cause disruption, not know-how and that is something that needs to be addressed.[109]

The guerilla combat of the post-Cold War era is open to a much larger pool of participants, whose cover is the anonymity and ubiquity of the "net." The general awareness that the critical infrastructure is critically, vulnerable, is as tempting to prospective attackers as it should be unnerving to its defenders and users. The tension creates a gambit for all international players. For state actors it may become a grand game of "chicken" to see who would launch a first strike. Many experts claim in preparation for that moment, some nation-states have been surveying the landscape to identify vulnerabilities in infrastructure systems of

[106] Cardenas, Alvaro A.
[107] Cornish, Paul, Livingston, David, Clemente, Dave, Yorke, Claire, "On Cyber War," Chatham House Report, November 2010, p. 28.
[108] Cohn, Mark, Unisys Corporation, correspondence, January 20, 2010.
[109] "Virtual Criminality Report 2009," p. 11.

power grids and communication networks. In the words of an expert quoted in the McAfee report nation-states are: "laying the electronic battlefield and preparing to use it."[110]

All the while there has been a lack of public debate and an attendant void of national strategy. Further hindering the debate is even the lack of a functioning lexicon to express a crime, attack, or a justifiable retaliation in cyberspace. Rules of engagement, established responses, and notions concerning deterrence or collective security are presently moot points, which cannot be resolved until there is a framework for guiding doctrine and action. During this failed process classified information is kept secret, goes unshared, or falls between the cracks. The procedure for laying out a strategy is further stifled by bureaucratic divides and the walls erected among the military, law enforcement, national governments, and global commerce. As this "dialogue of the deaf" persists, the want for action languishes. While much of the discussions go on behind the closed doors of government, the public and the private sector continue to be the target of daily assaults, and will so for the foreseeable future.

Another factor limiting our response is a lack of verifiable and quantitative data. Because of the reasons cited above, governments, corporations, and other victims are hesitant to come forth and admit to their victimization. As a result much of the data on cyber crime is merely anecdotal. Anecdotal data can lead to alarmism and encourage military response as the only option. Such action might satisfy our fears and rage, but may not be appropriate and almost surely cause greater instability.

On the other hand, calls for consensus building are well worn throughout our history. Without the incentive of a mighty stick or irresistible carrot, agreements are seldom achieve and their importunity goes on ignored when demands are based on nothing more than irrepressible optimism. At present there are no such self-regulating mechanisms or pressures to force stakeholders into a consensus. The to and fro between a Doomsday reckoning and Utopian fantasy appears to represent the state and direction of the discourse. Without some analytical discipline to assess the threat cyber crime and cyberterrorism pose to us all, our best hope for positive steps might be somewhere in between.

As to the overall challenges of cybersecurity, for additional interpretation it might be wise to recall a fictitious dialogue between Socrates and a Greek aristocrat, Meno. Meno poses a question to the philosopher: "How will you look for something when you don't know what it is?" The stated and ensuing exchange is referred to as "Meno's paradox." In the current arena of conflict solutions are elusive. The competition over political and economic control by state and non-state actors, the expanding web of criminals, terrorists, disgruntled workers, hacktivists, *et al*, add to global security's version of that paradox. The combatants are indistinct. Their motives are often vague. Demands are rarely offered. The shadowy world of failed states and opaque cyberspace, has resulted in changing roles for states, altered the impact of NGOs on civil society, and created new spheres of authority, with which we have no history or experience.

As an example, crime and terrorism traditionally, abided by separate ontological norms and dwelled in two diverse and lawless realms. However, in today's security environment, these realms are beginning to overlap and the consequences are evolving into a previously, unknown blend of potent danger and plight for governments, the private sector, and civil society. What emerges has been called the crime-terrorist nexus and has been quietly expanding for years. As it unfolds, it creates a serious dilemma for security, law enforcement professionals, and their functional responsibilities. Obscured by a complex of motivational factors and a constantly morphing threat vector, this new menace poses a severe challenge to established protocols and approaches to national security.

Even though motives sometimes differ, the *modus operandi* of these sundry actors can be similar if not identical. The intensification of the globalization process and the emergence of cyber crime and warfare have enabled illegal activity - whether motivated by material gain or ideological incentive. Despite the overwhelming advantage of resources of nation states, law enforcement agencies, and legitimate global commerce and industry, technology equilibrates all players with a level battlefield of accessible and comparative weaponry. Furthermore, transnational crime syndicates and international terrorist organizations often reflect the same efficiencies as multinational corporations due to the similarities of disaggregate organizational structures, agile and de-centralized chains of command, and technologically trained "staffs." Moreover, the connection between the criminals and terrorists is more common and apparent as terrorists become more entrepreneurial and resort to self-financing.

The array of failed states, the role of multinational firms, the obsolescence of traditional militaries, the exploitation of jurisdictional divides and legalities, and the opaque circumstances that influence attribution of attack and response, are only some of the issues that create and impact this shifting global security paradigm. The result is an opening within the global system for criminals and terrorists to nest, proffer, and are poised to exploit. As law enforcement agencies and national security organs grapple with questions of jurisdiction and mission ownership, a new threat takes shape that does not comfortably conform to previous patterns of activity, analysis, and protocols for response.

Inhibiting the ability to interdict is the lack of experience with this kind of threat, and the paucity of data that could help create predictive modeling methods and tools. These new opponents are a multivariate network of plotters. In some cases, they may be unrelated, stateless, and widespread – and in other cases, not. As a result, Meno's question becomes a troublesome and persistent dilemma for the security and defense communities as a simple, hypothetical query evolves into a somber, global concern.

[110] Ibid, p. 3