# THE AIR FORCE LAW REVIEW

## ARTICLES




**Volume 71** **2014**

# THE AIR FORCE LAW REVIEW

AFPAM 51-106

*The Air Force Law Review* is a publication of The Judge Advocate General, United States Air Force. It is published semiannually by The Judge Advocate General's School as a professional legal forum for articles of interest to military and civilian lawyers. The *Law Review* encourages frank discussion of relevant legislative, administrative, and judicial developments.

*The Air Force Law Review* does not promulgate Department of the Air Force policy. The opinions and conclusions expressed in this publication are solely those of the author and do not necessarily reflect the opinion of The Judge Advocate General, The Judge Advocate General's Corps, or any other department or agency of the U.S. Government.

The *Law Review* solicits contributions from its readers. Information for contributors is provided on the inside back cover of this issue.

Readers who desire reprint permission or further information should contact the Editor, *The Air Force Law Review*, The Judge Advocate General's School, 150 Chennault Circle, Maxwell Air Force Base, Alabama, 36112-6418. Official governmental requests for free copies, not under the depository program, should also be sent to the above address.

Cite this Law Review as 71 A.F. L. Rev. (page number) (2014).

---

*The Air Force Law Review* is available online at http://www.afjag.af.mil/library.

# THE AIR FORCE LAW REVIEW

**VOL. 71** **2014**

*Authority to publish automatically expires unless otherwise authorized by the approving authority. Distribution: members of The Judge Advocate General's Corps, USAF; judge advocates of the Army, Navy, Marine Corps, and Coast Guard; law schools; and professional bar association libraries.*

# AN INTEGRATED APPROACH TO CIVILIAN-MILITARY/ INTERAGENCY COUNTERTERRORISM CAPACITY BUILDING

*Lieutenant Colonel Stephen Keane* and Major Kenneth A. Artz***



* Lieutenant Colonel Stephen Keane, U.S. Marine Corps, B.A. University of Arizona (1994); J.D. William and Mary School of Law (2002); LL.M. The Judge Advocate General Legal Center and School (2006); currently Commanding Officer Marine Corps Security Force Battalion Bangor, Washington. Prior to this assignment he was a Marine Corps Fellow to the Department of Justice, National Security Division.

** Major Kenneth A. Artz, U.S. Air Force, B.A. University of Michigan (1988); J.D., Chicago Kent College of Law (1996); currently Chief of Media and Communications, HQ AF/JA. Prior to this assignment he was an Air Force Strategic Policy Fellow at the Department of Justice, National Security Division. He is a member of the State Bar of Michigan.

## I. INTRODUCTION

Foreign Counter Terrorism (CT) capacity building is vitally important to the National Security of the United States. Currently, a vast array of U.S. Government (USG) organizations, military and civilian, are involved with USG CT capacity building efforts. It is crucial for the national security of the United States for the USG to vastly improve and synchronize its efforts in the area of CT capacity building. Currently, and for a variety of reasons, many of USG CT capacity building organizations operate in a compartmentalized or "stove piped" fashion. A clear vision from a central USG authority detailing how such operations should be planned for and carried out would enhance the overall effectiveness of CT capacity building operations. Correspondingly, establishing formalized processes for interagency coordination across USG CT capacity building entities will ensure the USG's overall policy objectives in this area are executed consistently and clearly.

There are many USG organizations working towards the same goal of helping other countries fight terrorism but unity of effort is lacking among these disparate and often competing organizations. Clear assignment of roles, missions, and a centralized funding source from a USG central authority would greatly reduce unnecessary redundancy and ensure that the USG resources are most efficiently employed. Establishing formalized processes for inter-agency coordination across USG CT capacity building entities will ensure that the USG's overall policy objectives in this area are executed consistently and clearly. Ultimately, the USG should establish a CT capacity building framework that utilizes more centralized planning to enable better informed and resourced decentralized execution. Enhanced USG unity of effort, and less stove piping of effort, will translate into more credibly conveying the civil-military unity of effort approach to the entities the USG supports through CT capacity building operations.

President Obama recently recognized the need for increased unity of effort when he released Presidential Policy Directive-23 (PPD-23).[1] The public fact sheet to the April 2013 document states that a "collaborative approach, both within the United States Government and among allies, partners, and multilateral organizations"[2] is key to Security Sector Assistance (SSA), an area that encompasses foreign CT capacity building. PPD-23 further emphasizes the policy that unity of effort across the United States Government is essential, both in response to emergent opportunities and in support of long-term partnerships.[3]

First, this article will generally discuss the threat of terrorism to the United States (U.S.) and its allies. Next, this article will address the USG's current efforts at

[1] The White House, Fact Sheet: U.S. Security Sector Assistance Policy (Apr. 5, 2013), http://www.whitehouse.gov/the-press-office/2013/04/05/fact-sheet-us-security-sector-assistance-policy.

[2] *Id.*

[3] *See id.*

foreign CT capacity building. The third section will discuss ways to improve unity of effort in the USG in order to improve the USG's CT capacity building efforts. The fourth section will highlight the importance of establishing the rule of law in CT capacity building. Finally, the article will explore the importance of developing a common sense legal framework to deal with detainees seized during CT operations, a significant problem that can prevent successful CT capacity building operations.

## II. SITUATION

The purpose of CT capacity building is to prevent terrorists from harming the U.S. homeland or our allies. The terrorist organizations that the USG and its allies are countering may be grouped broadly into two general categories. Political terrorists use terrorism in an attempt to achieve a political goal such as the overthrow of a government. Ideological terrorists employ terrorism driven by extreme dogma and may be characterized by a desire to destroy certain forms of societal structure. Both types of terrorist organizations use violence as a weapon to achieve their goals. The use of terroristic violence is also employed, on increasing occasion, by states against their own citizens, insurgent groups and criminal gangs.[4]

Terrorist organizations typically seek to operate in areas where they have a certain degree of impunity such as remote border areas, ungoverned spaces, and perhaps even on the high seas and in cyberspace. Because they increasingly operate in areas that lack secure control by a state law enforcement apparatus, taking action to disrupt, dismantle, and defeat terrorist organizations presents a complex array of challenges. Terrorist organizations may utilize organized criminal activities or even otherwise legitimate business activities to finance terror operations. Terrorist groups have also been known to partner with organized criminal organizations for financing and support.[5]

Additionally, modern terrorist organizations are typically non-state actors that operate outside of traditional military organizations, and do not respect the customary law of armed conflict, the Geneva Conventions or basic human rights. Terrorist organizations may exercise control over territory, as well as elements of the police and/or government institutions. Terrorism poses risks to a state, and a capability for lethality and destruction, that may exceed the risks posed by more conventional criminal enterprises motivated primarily by financial gain. Many modern terrorist organizations possess a level of sophistication, training, and fire-power commensurate with a military organization. Terrorist organization capabilities

---

[4] Paul Shemalla, *Introduction*, *in* Fighting Back: What Governments Can Do About Terrorism 1-2 (Paul Shemalla ed., 2011) (referring to Thomas R. Mockaitis, *Terrorism, Insurgency, and Organized Crime*, *in id.* at 11).

[5] *Id.*

often exceed the capability of traditional law enforcement organizations to address independently.[6]

Post-conflict environments in particular lend themselves to exploitation by lawless groups and terrorists. In testimony to the Senate Armed Services Committee, Assistant Secretary of Defense Michael Sheehan described how:

> Despite the unique variables of each case there were constants, in fact all too familiar constants that faced us every time:
>
> • Law and order had completely broken down; there were no viable state institutions
> • Local police had stopped to function and were overtaken by military and paramilitary forces
> • There was no functioning judicial or penal system
> • There was minimal or no functioning civil society, such as a press or civic organizations
> • The country was bankrupt with no resources to hire and retain public workers including police
>
> Three consistent complaints were heard concerning the response to this challenge, most often coming from the military forces that were forced to move into the security vacuum created by broken police forces.
>
> • The training of the new force started too late and proceeded too slowly, emboldening trouble-making groups
> • There were not enough resources to train, equip or pay the police
> • There was a shortage of expertise in developing leaders and specialists
> • There was no judicial system to handle criminals and other trouble makers if apprehended by military or police units[7]

Clearly, the threat posed by terrorism is significant. Terrorism has been referred to as a problem that is complex and globalized, and more often than not related to other transnational threats.[8] The USG has been increasingly leveraging its vast resources for CT capacity building in an effort to address this complex problem.

---

[6] *Id.* at 1-6.

[7] *Building Police Forces in a Post-Conflict Environment: Testimony for the Senate Foreign Relations Committee*; Apr. 21, 2004 (statement of Michael A. Sheehan; Deputy Comm'r for Counter Terrorism, New York City Police Dep't; current Ass. Sec. of Def. for Special Operations & Low Intensity Conflicts), *available at* http://www.au.af.mil/au/awc/awcgate/congress/sheehan_post_conflict_police.pdf (last visited Apr. 30, 2014).

[8] Naureen Chowdhury Fink, *Meeting the Challenge: A Guide to United Nations Counterterrorism*

## III. CURRENT USG EFFORTS AT FOREIGN CAPACITY BUILDING

On September 11, 2001, the world awoke to the stark reality and threat of terrorism. Although the attack happened in the United States, the planning and the perpetrators all emanated from overseas. In response to the 9/11 attack, the USG has increasingly moved toward preventing terrorism abroad before the enemy can conduct terrorist operations in the United States.[9]

There is a substantial amount of foreign CT capacity building being conducted throughout the civilian and military components of the USG. The United States' military, intelligence, and law enforcement agencies each have been intensely involved in foreign CT capacity building efforts. The military's efforts are most evident in the higher profile conflicts of Iraq and Afghanistan. For example, in Afghanistan, as was done in Iraq, the U.S. military is working side by side with members of numerous USG executive agencies, such as the Department of State (DoS) and the Department of Justice (DOJ), to help establish a new legal system and rule of law regime that will stabilize and protect the supported country.[10]

In addition, the Department of Defense (DoD) runs the Defense Institute of International Legal Studies (DIILS), a joint military program which supports the CT capacity building mission by providing rule of law and counter-terrorism training and education to foreign military officers, legal advisors, and civilians.[11] In FY2011, DIILS conducted one-hundred thirty seminars all over the world with partner nations seeking rule of law training. Foreign military officers, legal advisors and pertinent civilians receive this important training to help set up or improve their military and civilian justice systems. The training, most importantly, builds accountability and transparency across their legal systems.[12]

Another DoD organization, the Defense Security Cooperation Agency (DSCA), directs and manages security cooperation programs and resources to promote U.S. interests and build allied and partner capacities. The DSCA focuses on promoting and supporting self-defense and coalition operations in the global war on terrorism, and promoting peace-time and contingency access for U.S. forces.[13]

---

*Activities* 3 (June 2012), http://www.ipinst.org/publication/policy-papers/detail/363-meeting-the-challenge-a-guide-to-united-nations-counterterrorism-activities.html.

[9] The White House, The National Security Strategy (2006), *available at* http://georgewbush-whitehouse.archives.gov/nsc/nss/2006/print/index.html.

[10] *See e.g.,* U.S. Dep't of State, Rule of Law Programs in Afghanistan, May 4, 2012, http://www.state.gov/j/inl/rls/fs/189320.htm; Dep't of State, *Strengthening Iraq,* May 19, 2011, *http://www.state.gov/r/pa/prs/ps/2011/05/163826.htm*; University of South Carolina, *Rule Of Law Collaborative,* http://www.rolc.sc.edu (last visited Apr. 30, 2014).

[11] About Defense Institute of International Legal Studies, https://www.diils.org/node/1455541/about (last visited Apr. 30, 2014).

[12] *Id.*

[13] *See* What is DSCA?, http://www.dsca.mil/sites/default/files/HRbrochure5.pdf (last visited Apr. 30, 2014).

Naval Post Graduate School in Monterrey, California, runs the Center for Civil-Military Operations (CCMR). CCMR has the mission of building partner capacity and improving interagency and international coordination and cooperation by addressing civil-military challenges. These challenges include: enhancing civil-military relations, supporting defense reform and institution building, improving peacekeeping and peace building operations, and combating terrorism. They have conducted programs for over one-hundred and fifty countries.[14]

The DoD has clearly shouldered the bulk of the mission in Afghanistan because of the dangerous security situation. Through the Combatant Command, CENTCOM, various departments within the DoD have combated terrorism in Afghanistan. Approximately 20 percent of SOCOM's 60,000 members are deployed to not only Afghanistan, but also 78 other countries around the world working with host nation militaries and other capacity building efforts.[15] Still, a lack of interagency unity of effort continues to plague operations.[16]

The U.S. Marine Corps, already a leader in capacity building operations by using Marine Expeditionary Units and Marine Special Operations Command's (MARSOC) Foreign Military Training Units to engage with foreign partners, is leaning forward in the drive to enhance interagency efforts on several fronts. The Marine Corps has established the Security Cooperation Group to execute and enable security cooperation programs, training, planning, and activities in order to ensure unity of effort. The Marines have also assigned several Field Grade Officers throughout the interagency via both fellowships and permanent assignments. Most notably the Marines have recently published the Marine Corps Interagency Integration Strategy which details how the Marines intend to work effectively within the interagency framework.[17]

Civilian agencies took more time to begin their foreign CT work than the DoD. However, in the past few years, progress has been made as a multitude of other government agencies have been engaged in CT capacity building as well.

---

[14] *See* Center For Civil Military Relations, http://www.ccmr.org/capabilities/ (last visited Apr. 30, 2014).

[15] Jr. Wilson, *SOCOM: The Year in Review*, Mar. 22, 2012, http://www.defensemedianetwork.com/stories/socom-the-year-in-review/.

[16] Randy George & Dante Paradiso, *The Case for a Wartime Chief Executive Officer Fixing the Interagency Quagmire in Afghanistan,* Foreign Aff, June 21, 2011, http://www.foreignaffairs.com/discussions/roundtables/does-the-afghan-war-need-a-ceo.

[17] USMC Interagency Integration Strategy (Marine Corps Service Campaign Plan) 2012-2020 Annex V (2013), *available at* http://www.marines.mil/News/Messages/MessagesDisplay/tabid/13286/Article/142496/usmc-interagency-integration-strategy-marine-corps-service-campaign-plan-2012-2.aspx.

On 4 January 2012, the DoS transformed the 30-plus year-old Office of the Coordinator of Counterterrorism into the Bureau of Counterterrorism to strengthen the Department's ability to carry out counterterrorism missions around the world.[18] The mission of the Bureau is to lead the Department's efforts to build foreign counter terrorism capacity abroad in the civilian sector and contribute efforts in the military and defense sectors.[19] The Bureau of Counterterrorism is also working with the newly established Strategic Counterterrorism Communications Initiative, which was established by a presidential Executive Order on 9 September 2011, to reinforce, integrate, and coordinate USG communications investments to combat terrorism and extremism around the world in an effort to counter the actions and ideology of al-Qaida and its affiliates.[20]

In 2011, the DoS spearheaded creating the Global Counter Terrorism Forum (GCTF). The GCTF has 29 founding member states and the European Union. The purpose of the GCTF is to build an international framework for dealing with 21st Century terrorist threats.[21] The GCTF has amassed $175 million to strengthen "counterterrorism-related rule of law institutions, and has developed best practice documents in rule of law, combating kidnapping for ransom and prison de-radicalization and disengagement." The GCTF is also in the process of developing two international training centers in the Middle East and North Africa region that will provide training in countering violent extremism and bettering rule of law institutions.[22] The GCTF's glaring weakness is in its neglect of the whole of government unified approach to CT capacity building.

The GCTF is also responsible for drafting and adopting the Rabat Memorandum on Good Practices for Effective Counter Terrorism Practice in the Criminal Justice Sector ("The Rabat Memorandum").[23] The Rabat Memorandum is an example of a "good practice" document that provides widely accepted investigative and prosecutorial good practices (e.g., development and use of cooperating witnesses, or the use of a form of plea bargaining) that are now being implemented world-wide as key components of a comprehensive CT legal regime. Unfortunately, the Rabat Memorandum is silent on the benefit of incorporating a civil-military interagency approach that incorporates military assets and capabilities into CT. Due to this significant omission, the memorandum falls short of a framework for basing CT capacity building efforts.

---

[18] Ambassador Daniel Benjamin, *Establishment of the Bureau of Counterterrorism*, Jan. 4, 2012, http:www.state.gov/j/ct/rls/rm/2012/180148.htm.

[19] U.S. Dep't of State, Ten Things You Should Know About The State Department's Bureau of Counterterrorism, http://www.state.gov/j/ct/rls/fs/fs/206185.htm (last visited Apr. 30, 2014).

[20] *Id.*, *see* Exec. Order No. 13584, 76 Fed. Reg. 56945 (Sept. 11, 2011).

[21] Exec. Order No. 13584.

[22] *Id.*

[23] Global Counterterrorism Task Force, The Rabat Memorandum on Good Practices For Effective Counter Terrorism Practice in the Criminal Justice Sector 1, http://www.thegctf.org/documents/10162/38299/Rabat+Memorandum-English (last visited Apr. 30, 2014).

According to the coordinator of the DoS's Bureau of Counterterrorism, Mr. Daniel Benjamin, the main goal of counterterrorism assistance to foreign countries is to help them move away from repressive approaches toward developing true rule of law frameworks.[24] Mr. Benjamin stated:

> [T]he better our partners are at using their criminal justice agencies to prosecute, adjudicate and incarcerate terrorists, the less they will resort to extralegal methods to crack down on a domestic threat. Moreover, our security benefits when countries deal with threats within their own borders—so that those threats don't balloon and demand that we act, and so we don't need to take the kind of dramatic steps that inevitably cause a backlash and radicalization. That is why we're working closely with our interagency partners—the Departments of Justice, Homeland Security, and Defense—to help foreign partners develop their law enforcement and justice sector institutions and to secure their borders.[25]

The DoS also runs the Anti-Terrorism Assistance (ATA) Program, which is the USG's foreign CT program for criminal justice agencies of partner nations. The ATA provides bomb detection assistance, crime scene investigation help, border, aviation and cyber security to our allies. In the past fiscal year, ATA trained more than 9,800 participants from more than 50 partner nations.[26] Increased coordination with military partners would undoubtedly strengthen this program.

As Mr. Benjamin mentioned above, the DOJ and Department of Homeland Security (DHS) are also playing an important role in CT operations. The DOJ deploys Resident Legal Advisors (RLAs) to U.S. embassies around the world to develop host country government and law enforcement sector capacity to deal with terrorism.[27] RLAs are generally posted for a minimum of 12 months and allow for development of strong partner relationships with host country agencies and officials together with a deeper understanding of local conditions, laws, and challenges as well as the establishment of the required trust needed to accomplish the mission.

The DOJ created the office of Overseas Prosecutorial Development, Assistance and Training (OPDAT) in 1991. OPDAT assists prosecutors and judicial personnel in other countries develop, among other things, a solid legal response to counterterrorism.[28] Through OPDAT, the DOJ has strategically positioned Resident Legal Advisors around the globe to assist in CT capacity building efforts.

---

[24] U.S. Dep't of State, Global Counterterrorism: A Progress Report, Dec. 18, 2012, http://www.state.gov/j/ct/rls/rm/2012/202179.htm.

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] Office of Overseas Prosecutorial Development, Assistance & Training, U.S. Dep't of Justice,

Additionally, the DOJ runs the International Criminal Assistance Investigative Training Assistance Program (ICITAP) which works with foreign governments to develop professional and transparent law enforcement institutions that protect human rights, combat corruption, and reduce the threat of transnational crime and terrorism. Although ICITAP is a DOJ program, the DoS, DoD, and U.S. Agency for International Development (USAID), among other federal agencies, fund ICITAP's programs. OPDAT and ICITAP would do well to coordinate their efforts with DIILS and CCMR.

The DHS recognizes the link between international security and the security of the United States. The DHS has personnel located in 75 countries working with the host nations to, among other areas, mentor foreign border agents, screen U.S bound maritime containers, and help identify known or suspected terrorist and other high risk travelers.[29]

The United Nations (U.N.) has also ramped up its CT capacity building efforts. For example, in 2006, the U.N. adopted a Global Counter-Terrorism Strategy which urges the states to: (1) address conditions conducive to terrorism; (2) prevent and combat terrorism; (3) build states capacities to prevent and combat terrorism; and (4) promote and protect human rights as a fundamental basis for CT efforts.[30] Further, the transnational nature of contemporary terrorism prompted the U.N. to develop an institutional architecture encompassing the Security Council and the thirty-one entities of the Counter-Terrorism Implementation Task Force (CTITF). Moreover, the U.N. Security Council adopted Resolution 1373 that can be considered the keystone to the U.N.'s response to global terrorism.[31] Resolution 1373 required all U.N. member states to pass legislation to help in the fight against terror. For example, it forces states to "criminalize the financing of terrorism and freeze assets of known terrorists and supporters, to refrain from providing active and passive support to entities or persons involved in terrorist acts, to prevent the movement and travel of known terrorists, and to intensify an accelerate law-enforcement cooperation to counterterrorism."[32]

Interagency capacity building efforts have increased significantly in the past decade. The amount of USG CT capacity building personnel working overseas, but not employed with DoD, has also increased substantially. Aside from the U.N., there are numerous Non-Government Organizations (NGOs) that are contracted by the United States and foreign governments to perform CT capacity building operations.

---

http://www.justice.gov/criminal/opdat/ (last visited Apr. 30, 2014).

[29] U.S. Dep't of Homeland Sec., Fact Sheet: DHS's International Footprint (Updated Dec. 12, 2011), http://www.dhs.gov/news/2011/12/02/fact-sheet-dhss-international-footprint.

[30] Fink, *supra* note 9 at 4.

[31] S.C. Res. 1373, ¶ X, U.N. Doc. S/RES/1373 (Sept. 28, 2011), http://www.un.org/docs/scres/2001/sc2001.htm.

[32] *Id.*

The need for unity of effort to fully leverage the potential of the USG to disrupt and defeat terrorist organizations through CT capacity building has never been greater. Yet, due to the sheer number of disparate agencies and a lack of centralized planning or control, unity of effort has become increasingly difficult to achieve.

## IV. IMPROVING UNITY OF EFFORT IN THE USG

With the explosion of resources and entities performing foreign CT missions, the struggle to put all of these agencies on the same page has become more difficult. Each organization has its own agenda and ideas as to how to accomplish foreign CT capacity building. Unity of effort is greatly lacking between the civilian agencies themselves as well as between the DoD and these same civilian agencies.

Former DoD Under Secretary of Defense for Policy, Michelle Flournoy, while at the Center For American Progress (CNAS), pointed out the importance of unity of effort:

> At the end of the day, unity of effort across the U.S. Government is not just about being more efficient or even more effective in operations. It can determine whether the United States succeeds or fails in a given intervention. Unity of effort is not just something that is nice to have; it is imperative.[33]

Ms. Flournoy cited to various efforts that the USG has attempted to achieve unity of effort, such as Presidential Policy Directives by Presidents Bill Clinton and George W. Bush, "pol-mil plans" and Combatant Commanders forming Joint Interagency Coordination Groups to bring interagency perspectives into their planning and operations. However, according to Ms. Flournoy, these efforts have merely been piecemeal approaches and have not solved the larger integration problem.[34]

PPD-23 is another attempt to improve unity of effort. The President's Policy emphasizes that unity of effort across the USG is essential, both in response to emergent opportunities and in support of long-term partnerships. A key tenant of the Policy is that a "collaborative approach, both within the USG and among allies, partners, and multilateral organizations" is necessary for successful Security Sector Assistance (SSA) operations, an area that includes CT capacity building.

PPD-23 attempts to unveil a new approach to CT capacity building or SSA strengthening its own capacity to plan, synchronize and implement SSA through

---

[33] *Achieving Unity of Effort in Interagency Operations: Hearing on Prospects For Effective Collaboration on National Security Before the House Armed Services Subcommittee on Oversight and Investigations 3, 110th Cong.* (2008) (statement of Michelle A. Flournoy, former Dep't of Def. Under Secretary of Def. for Pol'y), *available at* http://www.cnas.org/files/documents/publications/CNASTestimony_FlournoyHASCJan2908.pdf.

[34] *Id.*

U.S. whole of government collaboration between state security and law enforcement providers, governmental security and justice management and oversight bodies, civil society, institutions responsible for border management, customs and civil emergencies, and non-state justice and security providers.[35] The President's Policy is a new and much needed attempt at an improved coordination among USG agencies.

However, the entire CT capacity building effort will not be successful unless there is significant improvement in integrating military operations into CT capacity building efforts. Many countries require a robust military response, or even a combined military/civilian response to terrorist groups that control substantial territory, such as in Yemen, Mali, Pakistan, and Nigeria. However, the current USG CT capacity building efforts often fail to address how those countries should meld military operations with the criminal justice process in responding to terrorist threats and operations. This failure by the USG to articulate an overall CT capacity building framework leads to compartmented and disjointed CT capacity building effort that fails to address the reality of the danger posed by terrorists.

Specifically, with respect to integrating military forces with civilian agencies in a given operation, Ms. Flournoy highlighted the failures caused by a lack of unity of effort:

> In the last two decades, the United States has experienced some truly stellar military victories: rolling back Saddam Hussein's aggression against Kuwait in the 1991 Persian Gulf War, establishing a secure environment for the implementation of peace accords in the Balkans, driving the Taliban from power in Afghanistan in the wake of the September 11, 2001 terrorist attacks, and toppling Saddam Hussein's brutal regime in a matter of weeks.
>
> During the same period, however, the United States has also experienced some profound operational failures: from the successful effort to stabilize and rebuild war-torn Somalia to the failure to quell the insurgency and jump-start reconstruction early on in post-conflict Iraq. In such cases, the United States, and the international community more broadly, has had great difficulty translating military successes into the achievement of broader strategic objectives. Winning the peace has proven to be much more difficult than winning wars. While some of these operational failures may have stemmed from misguided policy or mistaken judgment, others have resulted from poor policy execution. In numerous operations, the United States has been unable to bring to bear all of its instruments of national power . . . in a coherent and effective campaign. In some cases, inadequate vertical integration meant that policy decisions

[35] *Id.*

> made in Washington did not translate into intended actions on the ground. In others, poor horizontal integration meant that the various agencies involved in execution operated independently of one another rather than as a team, yielding an uncoordinated and ineffective campaign.[36]

Ms. Flournoy also pointed out the source of the interagency failure lies primarily in the fact that the USG interagency, unlike the U.S. military, lacks sufficient capacity and doctrine to properly plan for operations as the interagency.[37]

The failures described by Ms. Flournoy can be sharply contrasted against CT successes that employed a strong civil-military/interagency approach to CT. For instance, after years of failure relying on unilateral civilian or military approaches to CT, both Colombia[38] and Northern Ireland[39] achieved success through carefully planned and coordinated civil-military/interagency CT operations.

The concept of improving unity of effort should be considered in three related contexts relative to CT capacity building. First, it should be recognized that the USG has made great strides in our own successful use of civil-military/interagency cooperation in CT operations. Second, a key component of CT capacity building is stressing civil-military/interagency cooperation. Finally, the best practice for stressing civil-military/interagency cooperation is designing comprehensive, multi-disciplinary CT capacity building packages, as a combined civil-military/interagency team, tailored to each country's needs.

Unity of command is a doctrine of military operations that ensures responsibility is located in one place. U.S. Army Field Manual 3-0 Operations defines it as one of nine Principles of War: "For every objective, ensure unity of command under one responsible commander."[40] Unity of command ensures that one person retains responsibility for the objectives and people that under his or her office, and at the same time, makes clear to everyone involved who is ultimately responsible.

> Unity of effort, though, may or may not be perfectly compatible with the responsibility that goes along with unity of command. Unity

---

[36] *Id.* at 1.

[37] *Id.* at 1-2.

[38] *See e.g.*, Juan Manuel Santos, *Afghanistan's challenges - Lessons from the Colombian Experience*, 2007 NATO Rev. 3; http://www.nato.int/docu/review/2007/Military_civilian_divide/Afghanistan_colombian_Challenge/EN/index.htm.

[39] *See e.g.,* Thomas R. Mockaitis, *The Irish Republican Army, in* Fighting Back: What Governments Can Do About Terrorism 332-49 (Paul Shemella ed., 2011); Thomas R. Mockaitis, *Low Intensity-Conflict: The British Experience*, 13/1 Conflict Quarterly 7, 8-9 (1993), *available at* http://journals.hil.unb.ca/index.php/JCS/article/viewFile/15092/16161.

[40] U.S. Dep't of Army, Field Manual 3-0, Operations, App. A, para. A-12, page 3 (27 Feb. 2008), *available at* http://downloads.army.mil/fm3-0/FM3-0.pdf.

> of effort implies a lack of responsibility because one person is not ultimately in charge; rather, unity of effort requires coordination. Either between the various U.S. government agencies themselves or between U.S. and international and local partners that are fundamentally necessary and important to achieving the civil-military goals associated with complex operations, coordination is as important as command. As most practitioners and analysts of complex operations would attest, unity of effort is extremely challenging because there is no single, ultimate "responsible commander."[41]

Without unity of command, if a particular agency does not want to carry out a task, they usually can figure out a way not to do it. Field Manual 3-0 states:

> Cooperation may produce coordination, but giving a single commander the required authority unifies action. The joint, multinational, and interagency nature of unified action creates situations where the military commander does not directly control all elements in the AO [area of operations]. In the absence of command authority, commanders cooperate, negotiate, and build consensus to achieve unity of effort.[42]

While having a unified commander over all aspects of USG CT capacity building efforts would be favorable from a planning and accountability perspective, the number of organizations across the interagency involved in CT capacity building, along with their separate chains of authority, make the prospect of unified command unlikely. Instead, an entity such as the National Security Council (NSC) should, through directed top down planning, move toward establishing greatly improved unity of effort. NSC effort in this arena would potentially be daunting because there are several systemic obstacles that generally inhibit achievement of unity of effort:

> Interagency coordination and cooperation continue to be a hot topic among analysts of governmental-security processes, particularly when dealing with issues surrounding terrorism. In many ways the plethora of study groups, think tanks and commissions that deal with improving interagency processes have become virtual cottage industries, producing a continuous spate of analyses that identify specific and general problems . . . .
>
> A number of factors complicate or potentially block effective interagency cooperation within any country's government . . . Internal

---

[41] Josh Jones, *Unity of Command and Unity of Effort in Complex Operations: Implications for Leadership*, July 20, 2010, http://inssblog.wordpress.com/2010/07/20/unity-of-command-and-unity-of-effort-in-complex-operations-implications-for-leadership/.

[42] *Id.;* Field Manual 3-0, *supra* note 41, at paras. A-12, A-13.

> dynamics involve the interests and characteristics of both government agencies and their individual members. It is fair to surmise not only that individuals will be drawn into different kinds of agencies according to their personality traits, but also that the path to success within a given agency typically can reinforce particular behaviors . . . this approach can result in disparate, self-reinforcing organizational cultures even within a larger department or ministry.
>
> On a more practical bureaucratic level, agencies almost inherently have competing interests that can pose real obstacles to coordination and cooperation. This translates into competition for funding. Given finite governmental resources, each agency has a vested interest in maximizing its influence and visibility within the government because doing so typically leads to increased funding . . . .
>
> To complicate matters further, the United States and some other countries have policies in place that deliberately preclude close interagency cooperation in some cases. These "firewalls" tend to be particularly strong between military and civilian agencies and between foreign and domestic intelligence operations, although since 2001 they have been reduced significantly within the U.S. government.[43]

One of the main policy guidelines of the PPD-23 is to strengthen the United States' own SSA capacity through a deliberate whole-of-government process. Past practice reveals the USG's weaknesses in getting past personal and institutional biases and impediments, which are crucial not only in the USG, but also in conveying effective CT capacity building approaches to foreign partners. One example would be the agencies of Tunisia. Its military is comprised largely of apolitical professionals who have demonstrated adherence to the rule of law and have ably filled gaps in civilian governance following the "Arab Spring." These gaps were created by overly politicized, and arguably corrupt and sectarian, civilian law enforcement institutions.[44] Therefore, it would be foolhardy not to include Tunisia's military in all CT efforts, including CT capacity building. Such an omission would be nearly comparable to marginalizing all former Baath Party members during the Iraq

---

[43] Lawrence E. Cline, *Interagency Decision Making*, 162, 162-165 *in* Fighting Back: What Governments Can Do About Terrorism 1-2 (Paul Shemalla ed., 2011).

[44] *See e.g.,* several articles on the Tunisia struggle, at Steven A. Cook, *The Calculations of Tunisia's Military*, Foreign Policy, Jan. 20, 2011, http://mideast.foreignpolicy.com/posts/2011/01/20/the_calculations_of_tunisias_military; Badra Gaaloul, *Back to the Barracks: The Tunisian Army Post-Revolution*, Sada, Nov. 3, 2011, http://carnegieendowment.org/2011/11/03/back-to-barracks-tunisian-army-post-revolution/6lxg; *Islamist Chaos has Tunisia Facing Threat of Military Coup*, World Tribune, Oct. 24, 2012, http://www.worldtribune.com/2012/10/24/islamist-chaos-has-tunisia-facing-threat-of-a-military-coup/; *Tunisia's Military Court Sentences Ben Ali to 20 Years for 'Incitement of Murder,'* Al Arabia News, June 13, 2012, http://english.alarabiya.net/articles/2012/06/13/220377.html.

reconstruction. The Tunisian military is the most stable, competent, and professional component of the state apparatus and should be leveraged as such.

There have been other interagency successes in security cooperation. Most of those successes, however, have been at the tactical and operational levels, and a result of *ad hoc* collaboration often based largely on personal relationships. Despite these successes, there has not been a coherent strategic vision or plan for CT capacity building, with clearly defined roles and responsibilities. One proposal calls for institutionalizing the successful operational approach at the strategic level. This would be pursued by producing a command structure on the DoD side of the civil-military relationship. Such a command would be tasked solely with conducting security cooperation missions:

> Over the past decade, the United States has conducted counterinsurgency (COIN) operations in two major theaters and participated in security cooperation (SC) operations worldwide to build partner capacity and defeat insurgents and terrorist networks. Successful COIN and SC operations hinge on the ability to fully integrate joint military and interagency capabilities to achieve strategic objectives. Recent operations in Iraq, Afghanistan, the Philippines, and elsewhere show that when SC operations are synchronized with military and interagency elements of national power, they can have a positive impact on security and stability. The current emphasis on SC at the strategic and operational levels reflects its significance; however, there is no Department of Defense (DoD) command responsible for integrated SC joint doctrine, training, interagency coordination, and worldwide force employment. Considering the importance of integrated SC operations and their relevance to the current global security environment, a new SC functional combatant command should be created that synchronizes joint, interagency resources and incorporates lessons learned during the past decade of SC and capacity building operations.[45]

Having a command structure at DoD makes sense because DoD has the most developed joint planning doctrine amongst the interagency. Utilizing DoD's planning expertise would go a long way towards achieving enhanced unity of effort. Moreover, the civilian component of USG CT capacity building operations should take steps to improve its planning process. A central USG authority, perhaps at the National Security Staff, should oversee the planning efforts of both the military and the civilian components to ensure that operations are carried out in accord

[45] Randal M. Walsh, *Security Cooperation: A New Functional Command Security Cooperation: A New Functional Command*, 64 Joint Force Quarterly 52, 53 (2012), *available at* http://www.dtic.mil/doctrine/jfq/jfq-64.pdf.

with a national strategy. This oversight should be designed to ensure collaboration, synchronization and efficient utilization of resources.

## V. THE IMPORTANCE OF THE RULE OF LAW IN FOREIGN CT CAPACITY BUILDING

One of the most important aspects of a successful foreign CT capacity building is developing a rule of law framework. The importance of this framework is to enable the countries to address their own terrorist problems before it becomes a problem of the U.S.

As stated in the Afghanistan Rule of Law and Law Enforcement magazine published by the Air Force Judge Advocate General's School, the U.S. military has long known the importance of establishing a rule of law in its international operations:

> What are now commonly referred to as "Rule of Law Operations" have been a part of American foreign policy since military personnel serving in the Philippines after the Spanish-American War began to introduce domestic legal concepts on the foreign islands in an effort to stabilize the growing society. Similar efforts were undertaken in both Germany and Japan post-WWII, and in Vietnam throughout the 1960s and 1970s. In the modern era, Rule of Law (ROL) programs have become increasingly more important, and vastly more common. The National Security Strategy says that "America's commitment to democracy, human rights, and the rule of law are essential sources of our strength and influence in the world." This guiding principle insures that the United States will continue to assist international partners in establishing open societies where no individual or institution is above the law, as doing so promotes global security and stability.[46]

Further, the goal of the DoS's CT assistance is to develop rule of law frameworks in countries that allow or breed terrorists. In PPD-23, the president acknowledged the importance of the rule of law when he stated the directive was aimed at "strengthening the ability of the United States to help allies and partner nations build their own security capacity, consistent with the principles of good government and rule of law."[47]

The best organization to help implement the rule of the law is through the use of a combined civil-military interagency team comprised of legal and law

---

[46] U.S. Air Force Judge Advocate General's School, *Introduction*, *in* Afghanistan Rule of Law and Law Enforcement, 2012.

[47] PPD-23, *supra* note 2.

enforcement experts from across the spectrum of government. As the terrorist target varies depending on factors such as the terrorist organization's geographic location, size, training and equipment, it makes sense to leverage USG and foreign expertise tailored to counter the specific target.

Terrorists are the main impediment to establishing a rule of law in many countries, as they often target the foundation of a rule of law regime by attacking law enforcement officials, prosecutors and judges, as seen in Iraq and Afghanistan. This is why it is crucial to establish working relationships between the military and these types of civilian agencies prior to beginning foreign CT.

## VI. LEGAL OPTIONS FOR CIVIL-MILITARY CT DETENTION AND PROSECUTION

The issue of what to do with suspected terrorists who are captured during CT operations can pose challenging concerns for the USG and our partners working to build CT capacity. To establish the rule of law, this issue must be resolved. This issue requires close civil-military coordination.

As mentioned above, many countries require a robust military response to terrorist groups who control substantial territory. This is the case currently in the on-going military operations in Mali. The French military, supported by several African nations as well as the Malian military, have had to use combat operations to remove Islamic terrorists from some major cities in Northern Mali.[48] The French military and the Malian forces resultantly faced the issue of what to do with terrorists captured during combat operations. Similarly, the United States faced significant issues on how to handle captured terrorists in Iraq and Afghanistan. This turned out to be a significant issue that impeded success. The detainees that are still being held in Guantanamo Bay are a testament to the importance of setting up a legal framework to detainees in CT operations.

Most terrorist acts may be prosecuted as crimes under statutes found in existing state penal codes, whether terrorist offenses are committed in peacetime or during military operations. During internationally-recognized war or hostilities short of war, terrorists may be prosecuted in accordance with the local penal code or under military jurisdiction by either a court-martial or military commission.[49] Preventative detention is also permissible under certain circumstances.[50] Analysis

---

[48] *See e.g.,* collection of articles on the Mali Conflict, at: The New York Times, http://topics.nytimes.com/top/news/international/countriesandterritories/mali/index.html (last visited Apr. 30, 2014).

[49] U.S. Army Judge Advocate General's School, Law of War Handbook 414 (2008).

[50] *See e.g.,* David Cole, *Out of the Shadows: Preventive Detention, Suspected Terrorists, and War*, 97 Cal. L. Rev. 693, 695 (2009).

of the detention and prosecution options available to states in their CT efforts must be a key component of every CT capacity building program.

A recent U.S. District Court for the District of Columbia decision, *U.S. v. Hamdan,* provides an informative discussion of the potential prosecutorial and detention options for governments dealing with captured terrorists. In 2001, Mr. Hamdan was captured in Afghanistan and determined to be a member of the al Qaeda terrorist organization. He was later transferred to the U.S. Naval Base at Guantanamo Bay, Cuba. Hamdan was detained at Guantanamo as an enemy combatant, and also accused of being an unlawful enemy combatant. The DC Circuit, while ruling on a separate issue related to the form of the charges, described in dicta a panoply of options:

> Our judgment would not preclude detention of Hamdan until the end of U.S. hostilities against al Qaeda. Nor does our judgment preclude any future military commission charges against Hamdan—either for conduct prohibited by the "law of war" under 10 U.S.C. § 821 or for any conduct since 2006 that has violated the Military Commissions Act. Nor does our judgment preclude appropriate criminal charges in civilian court. Moreover, our decision concerns only the commission's legal authority. We do not have occasion to question that, as a matter of fact, Hamdan engaged in the conduct for which he was convicted.[51]

It is important for a state to have options for detaining terrorist combatants. For example, the Supreme Court in *Johnson v. Eisentrager* stated,

> [t]he alien enemy is bound by an allegiance which commits him to lose no opportunity to forward the cause of our enemy; hence the United States, assuming him to be faithful to his allegiance, regards him as part of the enemy resources. It therefore takes measures to disable him from commission of hostile acts imputed as his intention because they are a duty to his sovereign.[52]

Arguably, a terrorist who is ideologically committed to attacking a state continues to pose a threat if released during a period of ongoing hostility and conflict. Hence, the states may have a need for detention choices that exceed the detention options normally used for conventional criminal cases.

International Humanitarian Law (IHL), also known as the Law of War and the Law of Armed Conflict, provides for detention of a combatant when a state of armed conflict exists and a member of the enemy force is captured and identified as

---

[51] Hamdan v. United States, 696 F.3d 1238, 1241-42, FN 1 (D.C. Cir. 2012).

[52] Johnson v. Eisentrager, 339 U.S. 763, 772-73 (1950).

an enemy combatant.[53] The detention power of a state is enhanced during periods of armed conflict because IHL recognizes the unique threats to state security posed by armed conflict. Prisoners of war (lawful combatants) may be detained for the duration of hostilities but, unless they have committed war crimes, are immune from criminal process for their acts of combat.[54] Unprivileged belligerents (unlawful combatants) may also be detained for the duration of hostilities but may also face trial for their criminal acts.[55] The authority to detain the combatants ends upon the cessation of hostilities; however, criminal incarceration may continue if a detainee has been prosecuted and convicted of a crime and remains serving a sentence.[56]

Law enforcement approaches to detention and prosecution pose challenges to effective CT because they are generally retrospective in nature and often fail to account for the unique evidentiary challenges present in complex CT operations. Still, law enforcement counter-terrorist operations that employ an efficient criminal justice process that respects the principles of rule of law and human rights, can offer a legitimate response to terrorism in the appropriate situation. When employed effectively, a criminal justice response to terrorism may serve to deescalate violence. Law enforcement approaches to CT potentially reinforce a society's commitment to the rule of law and human rights, even when under terrorist threats.[57]

The U.N. Office of Drugs and Crime recognizes the unique challenges of employing a law enforcement based approach to terrorism:

> An effective rule of law-based criminal justice response to terrorism involves more than the mere ratification and implementation of the universal instruments against terrorism. In addition to the appropriate laws, policies and practices, criminal justice practitioners need ongoing capacity-building and specialized training to enable them to respond effectively to the increasingly complex nature of terrorist crimes.[58]

The traditional criminal CT model, because of the substantive and procedural requirements, may be the most legitimate institution for long-term detention. The

---

[53] The Third Geneva Convention applies in an international armed conflict. Geneva Convention Relative to the Treatment of Prisoners of War, art. 4(A)(2), Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter Third Geneva Convention]. Common Article 3 applies even in a non-international armed conflict. *See* Adam Klein & Benjamin Wittes, *Preventive Detention in American Theory and Practice*, 2 Harv. Nat'l Sec. J. 85, 191 (2011).

[54] Third Geneva Convention, *supra* note 52*,* arts. 21, 118.

[55] Third Geneva Convention, *supra* note 52*,* art. 5.

[56] Third Geneva Convention, *supra* note 52*,* arts. 118, 119.

[57] U.N. Office of Drug & Crime, Handbook on Criminal Justice Responses to Terrorism 5 (2009), *available at* https://www.unodc.org/documents/terrorism/Handbook_on_Criminal_Justice_Responses_to_Terrorism_en.pdf.

[58] *Id.* at 33.

law enforcement CT model arguably may not, however, because of procedural and substantive requirements, comport well with the concept of preventive detention.[59]

National security law scholars have argued the military and civilian detention regimes have converged:

> During the past five years, the military detention system has instituted new rights and procedures designed to prevent erroneous detentions, and some courts have urged detention criteria more oriented toward individual conduct than was traditionally the case. At the same time, the criminal justice system has diminished some traditional procedural safeguards in terrorism trials and has quietly established the capacity for convicting terrorists based on criteria that come close to associational status. Each detention model, in short, has become more like the other. Despite convergence, neither model as currently configured presents a final answer to the problem of terrorist detention.[60]

It is becoming more accepted that even under the criminal justice approach, administrative preventive detention is effective because "such detention may be best suited to prevent continued fighting, and because states engaged in such conflicts are not expected to devote their law enforcement and other security resources primarily to the process of criminal prosecution and conviction."[61] "Human rights law permits states to detain persons posing serious security threats just as it permits states to detain persons who are awaiting deportation or who endanger public safety due to mental illness-not only through the criminal process, but also through systems of administrative detention." [62]

Recent USG successes in civil-military cooperation provide a model for CT capacity building efforts. For example, the April 2011 capture of Somali terrorist Ahmed Abdulkadir Warsame ("Warsame") may serve as a template for future military capture, detention, and transfer to civilian jurisdiction for prosecution in U.S. federal court.[63]

---

[59] *See* Robert Chesney & Jack Goldsmith, *Terrorism and the Convergence of Criminal and Military Detention Models*, 60 Stan. L. Rev. 1079, 1081 (2008); *see also* Monica Hakimi, *The Way Forward: International Standards for Detaining Terrorism Suspects: Moving Beyond the Armed Conflict-Criminal Divide*, 33 Yale J. INT'L L. 369, 386 (2008).

[60] Chesney & Goldsmith, *supra* note 59, at 1081.

[61] Hakimi, *supra* note 58, at 382.

[62] *Id*. at 388.

[63] Peter Finn, *Somali's Case a Template for U.S. as it Seeks to Prosecute Terrorism Suspects in Federal Court*, Washington Post, Mar. 30, 2013, *available at* http://www.washingtonpost.com/world/national-security/somalis-case-a-template-for-us-as-it-seeks-to-prosecute-terrorism-suspects-in-federal-court/2013/03/30/53b38fd0-988a-11e2-814b-063623d80a60_story.html.

According to Peter Finn's March 2013 *Washington Post* article, U.S. special operators captured Warsame in a raid off the coast of Yemen. Warsame was first held under the laws of war, pursuant to the Authorization for Use of Military Force.[64] For two months, he was in military detention and interrogated by the U.S. intelligence community on the naval vessel USS Boxer in the Indian Ocean. Then, President Obama's national security advisors decided to transfer Warsame from military detention to civilian detention. In June 2011, a team of FBI agents flew to the USS Boxer and gave Warsame a Miranda warning, advising him of his right to remain silent and his right to a lawyer. Warsame agreed to waive his rights and continued to answer questions.[65]

The "clean break" offered by the FBI agents to Warsame allowed for all admissions and evidence obtained through his subsequent statements to be available for use in his federal prosecution. Robert Chesney, blogger at the Lawfare blog run by the Brookings Institute, describes the Warsame case as a smart, hybrid approach because it combined military assets to capture, detain, and interrogate the terror suspect, with the maximum sustainability solution for long-term detention offered by the U.S. Federal Courts.[66] Professor Chesney also believes this case is a perfect case that "one need not take a one-size-fits-all approach in which you must either embrace a military or a law enforcement model from start to finish; these elements can and should work in combination in at least some instances . . . ." Chesney goes on to say,

> The lesson here is likely to be that what makes the most sense, from a CT policy perspective, is to ensure that the executive branch has the right array of options on hand, and that when free to use those options the government can bring them to bear in coordinated fashion that gives due account both to the imperative of acquiring intelligence and the goal of ensuring that a dangerous person can be incapacitated for the long term in the end.[67]

How the Warsame matter was coordinated is key to future CT operations. This type of working relationship between all the executive branches is needed for similar future successes.

---

[64] Authorization for Use of Military Force, Pub. L. No. 107-40, §2, 115 Stat. 224 (2001).

[65] *Id.*

[66] Robert Chesney, *Why No Period of Detention and Interrogation for Abu Ghaith, ala the Warsame Model?*, Lawfare, Mar. 7, 2013, http://www.lawfareblog.com/2013/03/detention-interrogation-abu-ghaith-warsam/.

[67] Robert Chesney, *Breaking News: Overseas Military Capture Extended Interrogation and Civilian Prosecution in New York City: U.S. v Warsame as the Model Case?*, Lawfare, July 5, 2011, http://www.lawfareblog.com/2011/07/breaking-news-overseas-military-capture-extended-interrogation-and-civilian-criminal-prosecution-in-new-york-city-us-v-warsame-as-the-model-case/ (last visited Apr. 30, 2014).

## VII. RECOMMENDATIONS

### A. General

There are several options for detention and prosecution under existing legal frameworks. Accordingly, CT operators need to be versed in available legal mechanisms, some of which may be outside the traditional options of their respective agencies. In particular, military forces must be trained to conduct CT operations with the insight that their efforts may in fact lead to civilian or military style criminal prosecutions. Civilian law enforcement experts bring a range of capabilities to the CT fight that often exceed what the military can provide. These capabilities include experience and expertise with financial and organized crime, seizure of assets through judicial systems, forensics, evidence security and evidence handling expertise and civilian prosecutorial experience and expertise. Additionally, with the prospect of criminal trials in CT, military forces must be versed in evidence collection and preservation. Moreover, they would ideally have the assistance of law enforcement experts at their disposal if not co-located with them during operations.

Law enforcement CT professionals need training with the insight that military forces are a key component of effective CT operations. Beyond sheer firepower for direct action, the military may provide improved intelligence, surveillance, and reconnaissance, advanced planning capacity, training expertise, personnel, equipment, and a more flexible legal methodology for the detention and prosecution of terrorists.

In contrast, failure to integrate civil-military/interagency assets can lead to failed operations and IHL and Human Rights violations. Elements of the military and civilian force may be become frustrated with lack of progress, confused roles and a lack of understanding of detention, prosecutorial options, and distrust of whether the legal system will properly secure captured detainees. This can lead to abuse of detainees and even extrajudicial killings and prisoner abuse.

### B. Specific

The following specific recommendations would enhance CT capacity building operations. These recommendations are designed to better organize a CT capacity building apparatus, improve planning, and foster synchronous USG resources.

(1) Develop and implement a USG plan for civil-military/interagency CT capacity building. The NSS, as required under PPD-23, must use its authority to initiate and oversee development of a comprehensive plan. Include in the plan the national strategy for CT capacity building, each agency's specific roles and responsibilities, and a framework for interagency cooperation and collaboration. Once the plan is issued, the same central

USG authority should oversee the plan's implementation to ensure the plan is implemented in accordance with its strategic intent. Funding oversight should be centralized at a high level to further promote compliance with the strategic intent.

(2) Include representatives from all the major CT capacity building agencies at DoD, DoS, DOJ, DHS, and others into the foregoing planning. Each department level organization should ensure coordination with their respective subordinate units that engage in CT capacity building so that realistic appreciation of the diverse equities located at the implementation level are considered during planning.

(3) Establish a rapidly deployable civil-military/interagency cadre that can deploy quickly for contingency operations and serve and the go-to organization for crisis action planning. Too much of the USG's CT capacity building civil-military/interagency coordination is done ad hoc and by happenstance. Developing a core group of civil-military CT experts with established relationships and a firm grasp on the national strategy will greatly improve CT capacity building programs, particularly when responding to a crisis or post-conflict situation.

(4) Implement USG interagency liaison programs. Liaisons perform details at offices outside their home agency. Performing such work should be deemed as career enhancing so as to encourage participation by top tier professionals. Resident liaisons will greatly facilitate interagency coordination and cooperation.

## VIII. CONCLUSION

The combined civil-military/interagency approach to CT has proven to be the most effective in the modern fight against terrorism. In the world of CT, the soldier, the police officer, the prosecutor, the investigating judge, and the prison guard each has a role; but, each also has a need to understand the role of the other CT professionals and when to engage them. The USG and its partners building CT capacity need to understand the resources available within the whole government and consequently bring the entire range of those resources to bear against terrorist adversaries. The most effective way to advocate the whole of government approach during CT capacity building operations is to establish a centralized planning framework for conducting these missions. Improved unity of effort amongst the USG will ultimately lead to greater results in CT capacity building operations.

# EXAMINING BLASPHEMY: INTERNATIONAL LAW, NATIONAL SECURITY AND THE U.S. FOREIGN POLICY REGARDING FREE SPEECH

*Lieutenant Colonel Eric M. Johnson**



* Lt Col Eric M. Johnson, Judge Advocate, United States Air Force (LL.M., The Judge Advocate General's Legal Center and School, Charlottesville, VA (2013); J.D., New England School of Law (2001); B.A., Virginia Polytechnic Institute and State University (1998)) is the Chief, Professional Outreach Division, The Judge Advocate General's School, Maxwell Air Force Base, Alabama. Previous assignments include Deputy Chief of Military Justice, Chief of Aviation Law and Deputy Chief of Operations Law, Headquarters Air Combat Command, Joint Base Langley-Eustis, Virginia, 2010-2012; Deputy Staff Judge Advocate, 11th Wing, Bolling Air Force Base, Washington, D.C., 2008-2010; Chief of General Law, Chief of Military Justice, 52d Fighter Wing, Spangdahlem Air Base, Germany, 2005-2008; Assistant Officer-in-Charge, Magistrate Cell, Joint Task Force 134, Camp Cropper, Iraq, 2007; Claims Officer, Deputy Chief of Military Justice, and Chief of Civil Law and Legal Assistance, 325th Fighter Wing, Tyndall Air Force Base, Florida, 2002-2005. Member of the bar of the Commonwealth of Massachusetts, the Court of Appeals for the Armed Forces, and the Air Force Court of Criminal Appeals. This article was submitted in partial completion of the Master of Laws requirements of the 61st Judge Advocate Officer Graduate Course.

## I. INTRODUCTION

In June 2012, a fourteen minute trailer to a movie titled "Innocence of Muslims" was posted to YouTube.[1] Though it received virtually no notice when initially made public, less than two months[2] later it was at the epicenter of a global controversy, a cause for terrorist groups seeking to target Western institutions, and the centerpiece of the debate over blasphemous speech and its legal protection. The movie, made in the United States with obvious low production values, makes numerous outlandish claims the Prophet Mohammed is (among other things) a homosexual, a child molester, and bloodthirsty.[3] This set off a series of anti-American riots throughout the Islamic world.[4]

Shortly after the demonstrations and riots in the Islamic world began over the "Innocence of Muslims" movie, a French satirical magazine published several cartoons depicting what is considered to be the Prophet Mohammed naked.[5] The director of the magazine pushed back against claims he was adding to the unrest, saying the magazine is "not really fueling the fire" but instead "comment[ing] [on] the news in a satirical way."[6]

Both of these events bring to a head the conflict between a fundamental human right, the freedom of expression, and blasphemy. United States law maintains a liberal protection of the right to freedom of expression protected in the U.S. Constitution's Bill of Rights.[7] International law, as delineated by the International Covenant on Civil and Political Rights (ICCPR), allows more restrictions to be placed on this right.[8] When should, if ever, the right to express opinions be curtailed in order to prevent blasphemy or the defamation of a religion?

---

[1] *The "Innocence of Muslims" Riots*, The N. Y. Times, Nov. 26, 2012, http://topics.nytimes.com/top/reference/timestopics/subjects/i/innocence_of_muslims_riots/index.html.

[2] *Id.*

[3] *Id.* The trailer can be viewed on YouTube at http://www.youtube.com/watch?v=qmodVun16Q4 (last visited Mar. 13, 2013). Subsequently, the full movie (over an hour in length) was also posted on YouTube. It was viewed at http://www.youtube.com/watch?v=X6s8eFkt90Q (last visited Mar. 13, 2013) but subsequently removed due to copyright claim.

[4] *See id.*; *see also* Rebecca Keegan, John Horn & Dawn C. Chmielewski, *Anti-Islam Film Contains Controversial Scenes by Mystery Director*, Los Angeles Times, Sept. 12, 2012, http://articles.latimes.com/2012/sep/12/entertainment/la-et-mn-antiislam-film-sparks-violence-20120912.

[5] Sharona Schwartz, *Naked Mohammed Cartoon Prompts French Embassy, School Closures across Middle East*, Blaze, September 19, 2012, http://www.theblaze.com/stories/french-satire-magazine-publishes-naked-mohammed-cartoons-and-now-officials-are-worried.

[6] Jim Bittermann, Pierre Meilhan & Holly Yan, *Free Speech or Incitement? French Magazine Runs Cartoons of Mohammed*, CNN.com, September 19, 2012, http://www.cnn.com/2012/09/19/world/europe/france-mohammed-cartoon/index.html.

[7] U.S. Const. amend. I.

[8] International Covenant on Civil and Political Rights, art. 19-20, Dec. 16, 1966, S. Treaty Doc. No.

Many followers of the Islamic faith take blasphemy, or the defamation of their religion, seriously and personally, and react violently when the west, in their mind, defames Islam. This blasphemous speech, or speech which defames religions, particularly Islam, is a source of global instability that can negatively affect the foreign policy interests and/or national security of the United States. In spite of this risk, the United States should continue to advocate for its liberal interpretation of the freedom of expression. There have been multiple incidents in the recent past where people have done things considered to be blasphemous in the Middle East and North Africa. As a result, violent riots have occurred across this strategically important region. Even though an anti-defamation of religion resolution may increase stability in this volatile region, the United States should not alter its current foreign policy. International law on the freedom of expression does not allow for restrictions on expression for this purpose, and the small benefit the United States would see is not enough to justify restricting the freedom of expression.

Part II of this article will attempt to define blasphemy and discuss blasphemy and defamation of religion as a source of instability, discussing examples of riots that have occurred after incidences of blasphemy across the world. It will also discuss the current U.S. foreign policy on the freedom of expression, and attempts to limit that right by prohibiting speech that defames religions. Part III will discuss the freedom of expression in international law, specifically discussing the Universal Declaration of Human Rights and the ICCPR. Part IV will compare and contrast the freedom of expression and blasphemy laws in the United States, Tunisia, Egypt, and Pakistan. Part V will discuss the U.S. approach to free expression and whether that approach advances our foreign policy interests. Part VI will conclude this article.

## II. BLASPHEMY AND THE INSTABILITY IT CREATES

Blasphemy and instability are inextricably linked together. Whether it is through purposeful action or accidental, when an action of someone from the western democracies is considered to be blasphemous to Islam, the *Quran*, or the Prophet Mohammed, violence has resulted.[9]

---

95-20, 6 I.L.M. 368 (1967), 999 U.N.T.S. 171 [hereinafter ICCPR]. Article 19, § 3 states:

> The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals. *Id.*

Article 20, § 2 states, "Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law." *Id.*

[9] *See infra* Part II.C.

A. What is Blasphemy?

This is a simple question without a simple answer. Blasphemy is defined in dictionaries as "the act of insulting or showing contempt or lack of reverence for God,"[10] or the "impious utterance or action concerning God or sacred things."[11] But the definition in the legal context is much more difficult. There is no clear, overarching legal definition of blasphemy.[12] Blasphemy means something different in every legal system in the world.[13] In fact, there is no common practice regarding blasphemy crimes in the Islamic states.[14] The crime of blasphemy has developed individually in each state based on varying practices that are usually unwritten and subjective.[15] Blasphemous words or acts have been the start of several riots in the past; as many Muslims feel an emotional attachment to the Prophet Mohammed and feel the need to protect him.[16]

Each religion may have a different interpretation of what is blasphemous. The question of what is blasphemy in Islam is not an easy one to answer. This is because the *Quran* does not define blasphemy.[17] One form of alleged blasphemy is any depiction of the Prophet Mohammed.[18] Some scholars have used the "hadiths," which are collections of sayings attributed to Mohammed, to create a definition of blasphemy; but even in the hadiths the definition depends on a person's interpretation.[19] The same holds true for the punishment of blasphemy. Neither the *Quran*

---

[10] *Blasphemy*, Merriam-Webster Dictionary, http://www.merriam-webster.com/dictionary/blasphemy (last visited Mar. 13, 2013).

[11] *Blasphemy*, Dictionary.com, http://dictionary.reference.com/browse/blasphemy?s=t (last visited Mar. 13, 2013).

[12] *See* Jeremy Patrick, *The Curious Persistence of Blasphemy*, 23 Fla. J. Int'l L. 187, 206 (2011).

[13] *See id.*

[14] *See* Paul Marshall & Nina Shea, Silenced: How Apostasy and Blasphemy Codes are Choking Freedom Worldwide 5 (2011).

[15] *See id.*

[16] *See infra* Part II.C, and Diana Kraft, *In Wake of Anti-Muslim Video, U.S. Religious Leaders Condemn Violence, Affirm Free Speech*, Haaretz.com, September 14, 2012, http://www.haaretz.com/news/features/in-wake-of-anti-muslim-video-u-s-religious-leaders-condemn-violence-affirm-free-speech-1.464931.

[17] Christa Case Bryant, *Anti-Muslim Video: What Muslim Teachings Say About Retribution for Blasphemy*, Christian Sci. Monitor, September 18, 2012, http://www.csmonitior.com/world/middle-east/2012/0918/anti-muslim-video-what-muslim-teachings-say-about-retribution-for-blasphemy.

[18] *See* Kraft, *supra* note 16.

[19] *Id.*; *see also* Primoz Manfreda, About.com Middle East Issues, *What is Blasphemy in Islam*, http://middleeast.about.com/od/religionsectarianism/a/What-Is-Blasphemy-In-Islam.htm (last visited Mar. 13, 2013). While this is true, there obviously does exist that which Muslims believe to be blasphemy. One list I found includes: denying the existence of Allah, drinking alcohol or stealing, throwing the Quran in the trash, writing text from the Quran in urine. *See Lesson 13: The Types of Blasphemy and Blasphemers*, Ass'n of Islamic Charitable Projects, http://www.aicp.ca/

nor the hadiths directly discuss the punishment for blasphemy.[20] The proponents of the strict Sharia religious law will argue that the punishment for blasphemy should be death.[21] However, at least one Islamic scholar has argued the *Quran* shows that no corporal punishment should be handed out for blasphemy and current Muslims go against the teachings of the *Quran*.[22]

The concept of blasphemy has currently taken on the label of "defamation of religion" when there have been attempts to limit freedom of expression in the international arena.[23] This could be considered a potentially larger concept as "defamation of religion" is not necessarily as tied to the insult of God or a sacred object/person as blasphemy.

B. The Middle East and North African States Strategic Importance to the U.S. and the U.S. Interest in Stability

To this day, the Islamic states, particularly the Middle East and North Africa, remain of vital strategic importance to the United States. As such, the United States foreign policy focus for at least the last decade has been on that region as the United States strives for stability, and recently democracy, in the region. The United States focus has mainly been due to the need for oil, to secure both access and a low price.[24] The United States has long had an oil addiction, and that need has been satiated mainly by foreign oil. Nearly sixty percent of the world's oil can be found in the Middle East region.[25] This is a region that has been, and remains, unstable and often dangerous.[26]

American national security interests were linked to the Middle East in 1980 by President Carter, with the announcement of what has become known as the Carter

---

Islamic-lesson/English/youth/the-islamic-education-series-book-5/chapter-of-belief/lesson-13-the-types-of-blasphemy-and-blasphemers/ (last visited Mar. 13, 2013). The lesson cites to verses from the *Quran* as support. *Id.*

[20] *See* Bryant, *supra* note 17.

[21] *See* Manfreda, *supra* note 19.

[22] Maulana Wahiduddin Khan, *Blasphemy in Islam: The Quran Does Not Prescribe Punishment for Abusing the Prophet*, Times of India, October 2, 2012, http://timesofindia.indiatimes.com/home/opinion/edit-page/Blasphemy-in-Islam-The-Quran-does-not-prescribe-punishment-for-abusing-the-Prophet/articleshow/16631496.cms.

[23] *See, e.g.*, Jeremy Patrick, *The Curious Persistence of Blasphemy*, 23 Fla. J. Int'l L. 187 (2011).

[24] *See* Bruce W. Jentleson, Andrew M. Exum, Melissa G. Dalton & J. Dana Stuster, *Strategic Adaptation: Toward a New U.S. Strategy in the Middle East*, Ctr. for a New Am. Security (June 2012).

[25] Nasser Momayezi, *Oil, the Middle East and U.S. National Security*, 1 Int'l J. Human. & Soc. Sci. 1 (Aug. 2011).

[26] *Id.*

Doctrine.[27] Through the Carter Doctrine, which has been enforced by every president since, the United States committed itself to using any means, including military force, to prevent outside forces from gaining control of the Middle East region.[28] The Carter Doctrine provided the rationale for the use of military force on numerous occasions in order to protect these interests. These include: United States assistance to Afghanistan during their war with the Soviet Union (1979–1989), Persian Gulf War (1990–1991), Somalia intervention (1992–1993), Operation Iraqi Freedom (2003–2010), and Operation Enduring Freedom (2001–present).[29] This doctrine has continually linked our interests, including foreign aid, diplomatic energy, and treasure, both in the form of money and lives, to this region for over thirty years.[30]

Oil is not the only American interest in the region, or the only reason that the region is strategically important. The region is also home to most of the important threats that the United States is facing today.[31] Many experts in this region have stated that the threat Iran poses is the biggest security risk currently facing the United States.[32] Other states in the region are of great strategic importance to the United States as well. Pakistan plays an extremely important strategic role in the region for the United States. Pakistan has a role in counter-terrorism, access to oil and regional political stability.[33] Egypt has long been the bellwether for the Middle East and North Africa, with a moderate Egypt the key to peace and stability in the region.[34] Tunisia's importance stems from their position as the "cradle of [the] Arab

---

[27] *See* Thanassis Cambanis, *The Carter Doctrine: A Middle East strategy past its prime*, Boston Globe, October 14, 2012, http://www.bostonglobe.com/ideas/2012/10/13/the-carter-doctrine-middle-east-strategy-past-its-prime-the-carter-doctrine-middle-east-strategy-past-its-prime/xkDcRIPaE68mFbpnsUoARI/story.html.

[28] *See id.*; *see also Cato Handbook for Policymakers*, CATO Inst. (7th ed. 2009), *available at* http://www.object.cato.org/sites/cato.org/files/serials/files/cato-handbook-policymakers/2009/9/hb111-52.pdf.

[29] Andrew J. Bacevich, *The Carter Doctrine at 30*, World Aff., Apr. 1, 2010, http://www.worldaffairsjournal.org/blog/andrew-j-bacevich/carter-doctrine-30.

[30] Cambanis, *supra* note 27.

[31] Jeffrey M. Jones, *In U.S. 6 in 10 View Iran as Critical Threat to U.S. Interests*, Gallup, February 16, 2010, http://www.gallup.com/poll/125996/View-Iran-Critical-Threat-Interests.aspx (stating a Gallup poll found that 61 percent of Americans believed that Iran's military is a threat to vital U.S. interests over the next decade).

[32] *See Iran, Hezbollah, and the Threat to the Homeland: Hearing before the H. Comm. On Homeland Sec.*, 112th Cong. (2012) (statement of Dr. Colin H. Kahl), and James Joyner, *America's Number One Geostrategic Threat?*, Atlantic Council, March 28, 2012, http://www.atlanticcouncil.org/blogs/new-atlanticist/americas-number-one-geostrategic-threat.

[33] *See* The National Strategy Forum, 20 Nat'l Strategy F. Rev. 1 (2011), *available at* http://www.nationalstrategy.com/Portals/0/documents/Spring%202011%20NSFR/The%20US-Pak%20Relationship.pdf.

[34] *See Strengthening the U.S.-Egyptian Relationship*, Council on Foreign Relations, May 2002, http://www.cfr.org/egypt/strengthening-us-egyptian-relationship-cfr-paper/p8666.

Spring," and important as to how the Arab Spring revolution continues to develop in that nation.[35]

This region is also the home of many of the most violent extremists, or terrorists, in the world.[36] A study completed in 1980 concluded two out of 64 terrorist groups were categorized as religiously motivated.[37] A repeat of that study in 1995 concluded 26 of 56 were religiously motivated, with the majority of those being motivated by Islam.[38] "The influence of religion cannot be underestimated when discussing forces contributing to Islamic extremism. Bin Laden and his followers see the current struggle with the West as a long, defensive, historical struggle blessed by Allah."[39] The rise of these Islamic extremist terrorist organizations, with their base in the Middle East and North Africa, has resulted in the United States focusing much of its global defense efforts on countering the terrorist threat, and that remains a top priority today.[40] Along with Iran, the other top threat to the United States remains al Qaeda.[41] One major aspect of President Obama's current defense strategy involves the "targeted, surgical" strikes to eliminate the al Qaeda leadership.[42] All these factors add together to make this region vitally important to the United States, both in terms of our economic needs (in terms of energy), and in terms of stopping global terrorism.

C. Instability Caused by Alleged Blasphemy

While there have been peaceful demonstrations in the Islamic world after an alleged blasphemous act has taken place, unfortunately violence and instability, in the form of riots or other breaches of the peace, have also frequently occurred.

In 1988, Salman Rushdie wrote a novel, "The Satanic Verses," prompting outrage among the Muslim world for its allegedly blasphemous content.[43] The book

---

[35] Jill Reilly & Alex Ward, *Cradle of Arab Spring Goes Up in Flames as Protesters Fire-omb Egyptian Presidential Palace and Youths Torch Cars at Funeral of Tunisian Leader*, Mail Online, Feb. 8, 2013, http://www.dailymail.co.uk/news/article-2275677/Cradle-Arab-Spring-goes-flames-protesters-bomb-Egyptian-presidential-palace-youths-torch-cars-funeral-Tunisian-leader.html.

[36] President Barack Obama, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, Jan. 3, 2012.

[37] John Moore, *The Evolution of Islamic Terrorism: An Overview*, Frontline, http://www.pbs.org/wgbh/pages/frontline/shows/target/etc/modern.html.

[38] *Id.*

[39] Steve A. Young, *A Basis for Middle East Islamic Extremism*, 2 Prof. Issues in Crim. Just. 9, 16 (2007).

[40] *See id.*

[41] Keith Johnson, *Al Qaeda Remains Top Threat to U.S.*, Wall St. J., June 30, 2011, http://online.wsj.com/article/SB10001424052702303763404576416191709848746.html.

[42] *Id.*

[43] *Perceived Insults to Islam Trigger Muslim Anger*, N. Y. Daily News, September 12, 2012,

triggered deadly riots in Islamabad, Pakistan and Mumbai, India.[44] Iran's Ayatollah Ruhollah Khomeini issued a fatwa (religious edict) calling for the death of Mr. Rushdie in 1989.[45] That edict still stands, and the reward for his murder has been raised to $3.3 million dollars.[46]

On May 9, 2005, Newsweek magazine ran a story alleging American interrogators at Guantanamo Bay, Cuba flushed copies of the *Quran* down a toilet in the detention center.[47] This story led to protests and riots across the Muslim world and resulted in at least 15 deaths.[48] One week later Newsweek retracted the story, which the Pentagon called "demonstrably false."[49]

In 2005 and 2006 a Danish newspaper published twelve cartoons depicting unflattering images of the Prophet Mohammed.[50] These cartoons generated violent protests across the Middle East and North Africa.[51] Over 200 people died, with many more injured, in these riots.[52] Each time the cartoons are reprinted or referenced, violence breaks out again. After one reprint al Qaeda claimed responsibility for bombing the Danish embassy in Pakistan in 2010.[53]

In 2010, Pastor Terry Jones, the head of a sixty-person congregation near Gainesville, Florida, threatened to host a "Burn a *Quran* Day" to mark the anniversary of the September 11, 2001 attacks.[54] This announcement led to large demonstrations in Afghanistan with "Death to America" chants, but no violence.[55] Pastor Jones later decided not to burn the *Qurans*.[56] Almost a year later, Pastor Jones did burn

---

http://articles.nydailynews.com/2012-09-12/news/33794945_1_muslim-backlash-danish-embassy-muslim-anger.

[44] *Id.*

[45] *Id.*

[46] *Iran Increases Price on 'Satanic Verses' Author Salman Rushdie's Head by $500K*, NBCNews.com, September 17, 2012, http://worldnews.nbcnews.com/_news/2012/09/17/13908002-iran-increases-price-on-satanic-verses-author-salman-rushdies-head-by-500k?lite.

[47] Whitney Eulich, *Blasphemy Riots: 6 Examples Around the World*, Christian Sci. Monitor—CSMonitor.com, http://www.csmonitor.com/World/Global-Issues/2012/0912/Blasphemy-riots-6-examples-around-the-world (last visited Apr. 18, 2014).

[48] *See id.*

[49] *Id.*

[50] *See* Jytte Klausen, The Cartoons That Shook the World (2009).

[51] *See* Eulich, *supra* note 47.

[52] *Id.*

[53] *Id.*

[54] *Id.*, *see also* Damien Cave & Annie Barnard, *Minister Wavers on Plans to Burn Koran*, N. Y. Times, September 9, 2010, http://www.nytimes.com/2010/09/10/us/10obama.html.

[55] *See* Eulich, *supra* note 47.

[56] *Id.*

a *Quran* after "putting the book on trial."[57] When video of the burning was posted online it led to violence in Afghanistan with at least nine people dead.[58]

In February 2012, it was discovered U.S. troops had burned copies of the *Quran* in a trash dump on a base in Afghanistan.[59] Local Afghan employees on the base evidently witnessed charred remains of the *Qurans* and passed information on the incident outside the base.[60] This led to violent protests involving thousands of people across Afghanistan, leading to at least twelve deaths.[61] While it was determined no service member had malicious intent, that fact had no effect on the riots.[62]

As discussed in Part I, the production of the "Innocence of Muslims" generated violence across the Middle East.[63] Egypt, Tunisia, Libya, Sudan and Yemen all experienced violence after the trailer was discovered on YouTube in September 2012.[64] Secretary of State Clinton attempted to make it clear to the world that the government of the United States had no part in the production or dissemination of the video, stating her personal opinion the video is "disgusting and reprehensible."[65] In spite of these statements, violence broke out across the region, with some of the worst violence in Yemen, where at least five Yemenis were killed.[66] The trailer caused angry mobs to gather at the U.S. Embassy in Egypt, where the mob breached the fortified walls of the embassy.[67] More angry demonstrators stormed the U.S. Embassy in Tunisia, leaving two people dead.[68]

---

[57] *Id.*

[58] Kevin Sieff, *Florida Pastor Terry Jones's Koran Burning Has Far-reaching Effect*, Wash. Post, April 2, 2011, http://www.washingtonpost.com/local/education/florida-pastor-terry-joness-koran-burning-has-far-reaching-effect/2011/04/02/AFpiFoQC_story.html.

[59] Eulich, *supra* note 47.

[60] *Id.*

[61] *Id.; see also Six Dead in Afghanistan Koran Burning Protests*, BBC News, February 22, 2012, http://www.bbc.co.uk/news/world-asia-17123464.

[62] Eulich, *supra* note 47; *see also* Sangar Rahimi & Alissa J. Rubin, *Koran Burning in NATO Error Incites Afghans*, N.Y. Times, February 21, 2012, http://www.nytimes.com/2012/02/22/world/asia/nato-commander-apologizes-for-koran-disposal-in-afghanistan.html.

[63] *See supra* Part I.

[64] *Widespread Protests Against U.S. Over Anti-Muslim Film*, CBS News.com, http://www.cbsnews.com/8301-202_162-57512841/widespread-protests-against-u.s-over-anti-muslim-film (last visited Nov. 25, 2012).

[65] Nasser Arrabyee, Alan Cowell & Rick Gladstone, *Turmoil Over Contentious Video Spreads*, N.Y. Times, September 13, 2012, http://www.nytimes.com/2012/09/14/world/middleeast/Mideast-turmoil-spreads-to-us-embassy-in-yemen.html.

[66] *Id.*

[67] *The "Innocence of Muslims" Riots*, *supra* note 1.

[68] *Id.*

D. U.S. Foreign Policy on the Freedom of Expression

The United States, as part of its foreign policy, advocates for expanded human rights around the world, including the freedom of expression. The U.S. foreign policy on the freedom of expression is to advocate for an expansive freedom similar to U.S. national law. This expansive freedom of expression would contain minimal restrictions.[69] The U.S. position was stated by Deputy Secretary Daniel Baer of the Department of State when he said, "we are consistent in advocating for a universal standard that has only the very narrowest of limitations on freedom of expression," and "we protect people's right to say pretty much all manner of speech. There are some limitations. They are very, very, very limited limitations."[70] This also happens to be the U.S. national law is on the subject; an expansive freedom with very few restrictions, and then only in limited circumstances.[71] In fact, in the same interview Mr. Baer specifically referred to the U.S. standard on incitement to violence as the only time speech should be restricted.[72]

The U.S. position on blasphemous speech is, not surprisingly, no different. The United States treats blasphemous speech as any other form of speech. The U.S. position is blasphemy should not be suppressed, and any suppression of blasphemy would be a threat to both the freedom of expression and the freedom of religion.[73]

E. Defamation of Religion Resolutions

Pakistan, acting on behalf of the Organization of Islamic Cooperation (OIC),[74] first proposed a resolution entitled "Defamation of Islam" to the United Nations Commission on Human Rights in 1999.[75] One of the stated goals of the OIC is to secure a restriction on blasphemy in the form of international law or resolutions from the United Nations.[76] The OIC proposed text of the resolution was solely focused on

---

[69] LiveAtState Interview with Daniel Baer, Deputy Assistant Sec'y, Bureau of Democracy, Hum. Rts., and Labor, Dep't of State, via interactive video platform (Sept. 27, 2012), *available at* http://www.state.gov/r/pa/ime/198332.htm.

[70] *Id.*

[71] *See infra* Part IV.A.

[72] Baer, *supra* note 69.

[73] *Id.*

[74] The OIC is an inter-governmental organization made up of fifty-seven states with a goal to protect the interests of the Muslim world which was founded in 1969. *About OIC*, http://www.oic-oci.org/oicv2/page/?p_id=52&p_ref=26&lan=en (last visited Dec. 1, 2012).

[75] Comm'n on Hum. Rts., Pakistan Draft Res., *Racism, Racial Discrimination, Xenophobia and all Forms of Discrimination*, U.N. Doc. E/CN.4/1999/L.40 (Apr. 20,1999).

[76] Robert C. Blitt, *Defamation of Religion: Rumors of Its Death Are Greatly Exaggerated*, 62 Case W. Res. L. Rev. 347, 353 (2011).

defamation of Islam.[77] The OIC draft resolution was not passed due to concern by the other members of the commission on the draft's sole focus on Islam.[78] However, a resolution entitled "Defamation of Religions" was adopted by the Commission.[79] While the title did change, the resolution continued to single out Islam by only mentioning that religion in the text of the resolution.[80] The U.N. Commission on Human Rights continued to adopt resolutions on the defamation of religions every year through 2005.[81] Once the Commission on Human Rights ceased to exist, the request for the resolution went to the General Assembly for consideration.[82] The General Assembly adopted the defamation of religions resolutions for the years 2005–2010.[83] While the United States has consistently opposed these resolutions, the resolutions passed the General Assembly or the Commission on Human Rights by large margins in the early years.[84] In 2008, the resolution only passed by a plurality.[85] Recently, states have become more educated about what the defamation of religions resolutions mean; specifically, their relationship and danger toward the infringement of human rights, especially the freedom of religion and the freedom of expression.[86] This led to the United Nations Human Rights Council (UNHRC) (the successor of the Commission on Human Rights) adopting a resolution in 2011 that does not include the concept of defamation of religion.[87] This resolution, UNHRC

---

[77] L. Bennett Graham, *Defamation of Religions: The End of Pluralism?*, 23 Emory Int'l L. Rev. 69, 70 (2009).

[78] *Id.*

[79] C.H.R. Res. 1999/82, U.N. ESCOR, 55th Sess., Supp. No. 3, U.N. Doc. E/CN.4/1999/167, at 280 (Apr.30, 1999).

[80] *See* Graham, *supra* note 77; *see also* Jaime Contreras & Rosa Maria Martinez De Codes, *Cultural and Legal Issues Concerning Defamation of Religions*, *in* Fides et libertas 2008-2009 31, 38 (2008-2009). While written broadly enough to apply to any religion, the only religion mentioned in the resolutions is Islam. *Id.*

[81] C.H.R. Res. 2005/3, U.N. ESCOR, 61st Sess., Supp. No. 3, U.N. Doc. E/CN.4/2005/135, at 21 (Apr. 12, 2005); C.H.R. Res. 2004/6, U.N. ESCOR, 60th Sess., Supp. No. 3, U.N. Doc. E/CN.4/2004/127, at 28 (Apr. 13, 2004); C.H.R. Res. 2003/4, U.N. ESCOR, 59th Sess., Supp. No. 3, U.N. Doc. E/CN.4/2003/135, at 34 (Apr. 14, 2003); C.H.R. Res. 2002/9, U.N. ESCOR, 58th Sess., Supp. No. 3, U.N. Doc. E/CN.4/2002/200, at 56 (Apr. 15, 2002); C.H.R. Res. 2001/4, U.N. ESCOR, 57th Sess., Supp. No. 3, U.N. Doc. E/CN.4/2001/167, at 47 (Apr. 18, 2001); C.H.R. Res. 2000/84, U.N. ESCOR, 56th Sess., Supp. No. 3, U.N. Doc. E/CN.4/2000/167, at 336 (Apr. 26, 2000) [hereinafter Defamation Resolutions]. The resolutions remained written broadly enough to capture any religion, but with the only religion mentioned by name being Islam.

[82] *See* Graham, *supra* note 77, at 71.

[83] *See id.* and G.A. Res. 61/164, U.N. Doc. A/RES/61/164 (Dec. 19, 2006); G.A. Res. 62/154, U.N. Doc. A/RES/62/154 (Dec. 18, 2007); G.A. Res. 63/171, U.N. Doc. A/RES/63/171 (Dec. 18, 2008).

[84] *See* Graham, *supra* note 77, at 71-72.

[85] *Id.*

[86] *See id.*

[87] Human Rights Council Res. 16/18, Combating intolerance, negative stereotyping and stigmatization of, and discrimination, incitement to violence and violence against, persons based on religion or belief, 16th Sess. April 12, 2011, A/HRC/RES/16/18 (April 12, 2011).

Resolution 16/18, focuses on the combating of intolerance and negative stereotyping of religions instead of focusing on the defamation of any religions, making the resolution more in line with the freedom of expression.[88] Concern has still been expressed by some critics, even with this more moderate resolution, that Resolution 16/18 does not repudiate the concept of defamation of religion.[89]

In the international arena, the concept defamation of religion has eluded definition despite many resolutions passed by the United Nations General Assembly and its committees and subcommittees on the subject. This is one of the problems with the Defamation Resolutions. No meaning is given to the term "defamation of religions," and the resolutions are all written in vague, broad terms.[90] Clearly, this creates problems for enforcement. What are states to prohibit? What should states strive to eradicate? What religions are included? The only religion mentioned in many of the resolutions was Islam,[91] but would this also include non-mainstream religions? The U.S. Commission on International Religious Freedom (USCIRF), an independent bipartisan federal government entity, stated in their 2010 annual report to Congress:

> Aside from Islam, the resolutions do not specify which religions are deserving of protection, or explain how or by whom this would be determined. The resolutions also do not define what would make a statement defamatory to religions or explain who decides this question. For its part, the OIC appears to consider any speech that the organization, or even a single cleric or individual, deems critical of or offensive to Islam or Muslims to automatically constitute religious defamatory speech.[92]

Perhaps that was never the point of the resolutions, since these resolutions are non-binding there is no mandatory action states are required to take. The vagueness of the

---

[88] *See id.*; *see also* Press Release, U.S. Comm'n on Int. Religious Freedom, USCIRF Welcomes Move Away from "Defamation of Religions" Concept (March 24, 2011), *available at* http://www.uscirf.gov/news-room/press-releases/3570.html (last visited Mar. 13, 2013).

[89] *See* Blitt, *supra* note 76, at 371-78. "By failing to decisively invalidate the chimera of defamation of religion, the UN has allowed the OIC to advocate its continued legality, including by openly asserting that implementation of Resolution 16/18 is one possible 'alternative approach' to achieving the end goal of shielding religious beliefs from criticism and insult." *Id.* at 377.

[90] *See* Defamation Resolutions, *supra* note 81; *see also* Contreras & De Codes, *supra* note 80

> In such UN Resolutions there are a number of provisions that condemn defamation, underlining the intensification of the campaign of defamation of religions; they stress the connection between defamation of religions and incitement to religious hatred; they mention that defamation of religions could lead to social disharmony and violations of human rights—but there is not one single definition of 'defamation of religions.' *Id*.

[91] *See id*.

[92] U.S. Comm'n on Int. Religious Freedom, 2010 Annual Report, 336 (2010).

resolutions does give room for the OIC states to argue anything could be defaming Islam, and should be restricted. Perhaps the point was to begin the prohibition of defamation of religions on its way down the path to customary international law, which would then become binding on all states.[93]

The use of defamation of religions is also problematic because the traditional concept of defamation is meant to protect individuals from falsehoods, but not organizations.[94] In order to defend oneself in a defamation suit, if one is able to prove that the statement made is true, then that truth serves as an absolute defense.[95] This makes the application of this concept to religions impossible, because by its very nature religions are not provable to an objective standard.

Further, the genesis of resolutions prohibiting defamation of religion arguably introduces other ways to infringe upon human rights, most notably the freedom of expression. These limitations would not be in accordance with current international law as it stands regarding the freedom of expression.[96]

## III. FREEDOM OF EXPRESSION IN INTERNATIONAL LAW

The notion of a human right to the freedom of expression, or the freedom of speech, is not a recent invention. One of the first peoples to accept a freedom of speech was the ancient Greek city-state of Athens in approximately the year 500 B.C.[97] The freedom of speech, while not written into the Athenian constitution, was widely accepted among all Athenians.[98] In a tragic irony, Athens, the first democracy and creator of the freedom of speech, put the philosopher Socrates on trial for what amounted to his use of his freedom of speech.[99]

The freedom of expression continued to slowly develop over the centuries with supporters such as John Stuart Mill, John Milton, and Thomas Jefferson.[100] However, it was not until the year 1789 that the freedom of speech was codified

---

[93] *See* Patrick, *supra* note 23, at 192 (citing Liaquat Ali Khan, *Combating Defamation of Religions*, Am. Muslim, Jan 1, 2007, *available at* http://www.theamericanmuslim.org/tam.php/features/articles/combating_defamation_of_religions (last visited Mar. 13, 2013); *see also* Blitt, *supra* note 76.

[94] *See* Graham, *supra* note 77, at 75.

[95] *Id.* at 76.

[96] Jeroen Temperman, *Freedom of Expression and Religious Sensitivities in Pluralist Societies: Facing the Challenge of Extreme Speech*, 2011 BYU L. Rev. 729 (2011); *see also* ICCPR, *supra* note 8.

[97] Robert Hargreaves, The First Freedom: A History of Free Speech 1 (2002)

[98] *See id.* at 1-21.

[99] *Id.* at 15. Socrates was charged with corrupting the young and impiety. He was found guilty and sentenced to death, which was accomplished by his consumption of poison hemlock. *Id.* at 14-21.

[100] *See generally id.* (giving an overview of the development of the freedom of speech through history).

into a country's constitution, in the form of France's Declaration of the Rights of Man.[101] The Declaration proclaimed, "The free communication of ideas and opinions is one of the most precious of the rights of man. Every citizen may, accordingly, speak, write, and print with freedom, but shall be responsible for such abuses of this freedom as shall be defined by law."[102] That was soon followed in 1791 by the First Amendment to the United States Constitution which stated "Congress shall make no law . . . abridging the freedom of speech, or of the press . . . ."[103] After this point in history, the freedom of speech began to gain more traction, and is now considered a basic human right found in countries all over the world.[104]

After the devastation of World War II, the international community came together for the first time to begin drafting international agreements that listed and protected basic human rights.[105] Many of these documents received inspiration from a 1941 speech by President Franklin D. Roosevelt. In that speech he spoke of human rights containing the freedom of expression, freedom of faith, freedom from want, and freedom from fear.[106] The two most important international agreements on human rights, the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, will be discussed in detail below.[107]

### A. The Universal Declaration of Human Rights

The horrors committed during World War II are of such nature that it is difficult to comprehend how and why they could happen. As one commentator said, "[a]fter World War II, different peoples of the world were perhaps more united than at any time before or since on the need for a practical enforceable international morality to avoid a recurrence of war and its accompanying mass atrocities."[108]

---

[101] William Magnuson, *The Responsibility to Protect and the Decline of Sovereignty: Free Speech Protection Under International Law*, 43 Vand. J. Transnat'l L. 255, 277 (2010).

[102] Declaration of the Rights of Man and the Citizen para. 11 (France 1789).

[103] U.S. Const. amend. I.

[104] *See* Magnuson, *supra* note 101.

[105] *See id.*

[106] The Universal Declaration of Human Rights: A Commentary 10 (Asbjorn Eide, Gudmundur Alfredsson, Goran Melander, Lars Adam Rehof, Allan Rosas & Theresa Swinehart eds. 1992).

[107] While not discussed in this article, regional human rights treaties often also protect the freedom of expression. Some of the more important regional treaties include the European Convention, American Convention on Human Rights, and the African Charter on Human Rights. Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 22 [European Convention], Organization of American States, American Convention on Human Rights, Nov. 22, 1969, O.A.S.T.S. No. 36, 1114 U.N.T.S. 123, and African Charter on Human and Peoples' Rights, June 27, 1981, 21 I.L.M. 58, OAU Doc. CAB/LEG/67/3 rev. 5, *entered into force* Oct 21, 1986, 21 I.L.M. 58.

[108] Roger Normand & Sarah Zaidi, Human Rights at the UN: The Political History of Universal Justice 196 (2008).

The World War II atrocities laid the groundwork for the post-war world where the international community would focus on protecting human rights.

In 1946, the U.N. Human Rights Commission was formed, with their first task to draft a bill of human rights.[109] The Commission, made up of representatives of 18 member states, unanimously elected Eleanor Roosevelt, the late President Franklin D. Roosevelt's wife, as chairman of the commission.[110] The appointment of Eleanor Roosevelt brought great prestige to the commission, both because of the stature of her late husband and her own effectiveness in advocating humanitarian causes.[111] Mrs. Roosevelt has been stated to be "one of the chief assets of the Human Rights Commission in the early years."[112] Peng-chun Chang, from China, was appointed as the vice chairman of the commission, with Charles Malik, from Lebanon, appointed as the rapporteur (secretary).[113]

The Commission first met in January 1947, with the process for drafting a Universal Declaration of Human Rights (UDHR) proceeding rapidly. The Commission went through several drafts before a final draft was ready to present to the General Assembly for a vote in December 1948.[114] The General Assembly first took each article in the proposed UDHR individually, voting on each one.[115] Amazingly, twenty-three of the thirty articles were approved without any nay votes or abstentions, with the remaining overwhelmingly supported.[116] When the entire UDHR was put to the General Assembly for a vote it was approved unanimously, with only 9 abstentions.[117]

---

[109] Mary Ann Glendon, A World Made New 31 (2001).

[110] *Id.* at 32-33.

[111] *Id.* at 33.

[112] *Id.*

[113] *Id.*

[114] *See* Normand & Zaidi, *supra* note 108. For a complete history of the drafting process (including copies of the various draft declarations), with a focus on Eleanor Roosevelt's participation and influence, *see* Glendon, *supra* note 109.

[115] *See* Glendon, *supra* note 109, at 170.

[116] *Id.* Article 19, the freedom of expression article, received seven nay votes. *Id.* at 169.

[117] H. Lauterpacht, International Law and Human Rights 402 (1950). The nine abstentions were the Soviet Union, Belorussia, Czechoslovakia, Honduras, Poland, Ukraine, Yugoslavia, Saudi Arabia, and South Africa. *Id.* South Africa abstained because the Declaration stood apart from their apartheid regime. Saudi Arabia's reasons included the failure to include a reference to God in the Declaration and the failure to completely address colonialism and self-determination, and finally that the Declaration was based too much on Western ideals and culture. The remaining communist states based their abstentions on the failure of the Declaration to recognize the interdependence of the individual and the state, the failure to address the economic and social conditions in states, and did nothing to prevent fascism. *See* Normand & Zaidi, *supra* note 108, at 193-94.

The major downside to the passing of the UDHR is the declaration has no legal effect and no means of enforcement.[118] Nearly all members of the Commission "gloried in the profound significance" of the document that they were creating, yet still declined to give the declaration any legal effect.[119] This was also the position of the United States, with Mrs. Roosevelt articulating the declaration was not a legislative document, and was to only have moral persuasive authority.[120] "[I]t is not a treaty; it is not an international agreement. It is not and does not purport to be a statement of law or of legal obligation. It is . . . to serve as a common standard of achievement for all peoples of all nations."[121] The Declaration was even dismissed by the American ambassador to the United Nations as a "letter to Santa Claus."[122] The representatives for France and Belgium were alone in asserting some sort of legal authority for the declaration, but even that support was inconsistent.[123]

While the UDHR is merely a persuasive authority, not by its terms legally binding on any nation, it has had a large impact on states around the world. At this point, many (if not all) of the human rights proposed by the UDHR can be considered to be customary international law, which is binding on all nations.[124] One commentator expressed the truly universal acceptance of the UDHR by stating that it has "become a part of the common law of the world community; and, together with the Charter of the United Nations, it has achieved the character of the world law superior to all other international instruments and to domestic laws."[125]

Because of this universal acceptance, the UDHR is the single most important document produced in support of human rights. The UDHR has been hailed by many commentators as one of the greatest achievements of the United Nations.[126] The President of the General Assembly stated at the time,

> It was the first occasion on which the organized community of nations has made a declaration of human rights and fundamental freedoms. That document was backed by the authority of the body of opinion of the United Nations as a whole, and millions of people,

---

[118] *See* Lauterpacht, *supra* note 117, at 397.

[119] *Id.*

[120] *Id.* at 399.

[121] *Id.* at 398-99.

[122] Hargreaves, *supra* note 97, at 271.

[123] *See id.* at 402.

[124] *See* Hurst Hannum, *The Status of the Universal Declaration of Human Rights in National and International Law*, 25 Ga. J. Int'l & Comp. L. 287 (1996).

[125] Louis B. Sohn, *The Universal Declaration of Human Rights*, 8 J. Int'l Comm'n Jurists 17, 26 (1967).

[126] *See* Lauterpacht, *supra* note 117, at 394.

> men, women, and children all over the world, many miles from Paris and New York, would turn to it for help, guidance and inspiration.[127]

While some of the comments at the time of the passing of the UDHR were very effusive and clearly full of hyperbole,[128] the General Assembly President's comment has stood the test of time and seems to be supported by history. The UDHR has become the "primary inspiration" for all human rights documents, a "reference point" for all human rights discussions, and a wide ranging moral and persuasive authority against all whom decide to violate human rights.[129]

Many countries have incorporated provisions of the UDHR into their constitutions or their own bill of rights.[130] Even where provisions of the UDHR were not directly incorporated into a state's constitution or bill of rights, the UDHR served as the basis and inspiration for these documents. It has even had influence in the U.S. legal system.[131] It has been estimated over ninety states' constitutions have been inspired by the UDHR or served as the model for them.[132] Clearly the impact this document had on human rights cannot be overestimated.

An important question regarding the UDHR is whether the Declaration only contains what can be called "western" values and cultural recognition, or if it is more multi-cultural. If the human right you are espousing is considered only "western," for instance, will it have acceptance in the east?[133] This philosophical discussion

---

[127] *Id.* at 395.

[128] For example, the representative from Paraguay said, "it would shed a light on the way man had to tread to reach happiness," with the representative from Haiti calling it the "greatest effort yet . . . to give society . . . moral foundations," and the representative from Syria saying that the people's "aim had been reached by the United Nations." *Id.* at 395-396.

[129] Glendon, *supra* note 109, at xvi.

[130] Magnusson, *supra* note 101, at 279.

[131] *See* Tai-Heng Cheng, *The Universal Declaration of Human Rights at Sixty: Is it Still Right for the United States?*, 41 Cornell Int'l L.J. 251, 254 (2008).

[132] Glendon, *supra* note 109, at 228.

[133] Two of the main camps in this debate are the Relativists and the Universalists. A relativist believes that "cultures manifest so wide and diverse a range of preferences, morality, motivations, and evaluations that no human rights principles can be said to be self-evident and recognized at all times and all places." Therefore, if a certain right did not come from a particular culture, then the validity and applicability will be in doubt. Michael Goodhart, *Origins and Universality in the Human Rights Debate: Cultural Essentialism and the Challenge of Globalization*, 25 Hum. Rts. Q. 935, 939 (2003).

In contrast, a Universalist believes that "some moral judgments are universally valid," most believing that the rights embraced in the UDHR and other international treaties are those that are universally valid. The claims derive from arguments that some rights transcend culture and are valid arguments regardless of where it first appears based on things like natural law, justice, equality and respect. *Id.* at 940.

plays a direct role in the discussion of the freedom of expression and blasphemy and could affect the acceptance that the Declaration receives in other parts of the world. It also drives straight to the point of whether the Declaration is truly "universal," as it purports to be. When the UDHR was passed by the General Assembly, the U.N. comprised less than one-third of its current member states.[134] During the drafting process the United States exercised dominant influence on much of the discussion and drafting on most of the key decisions on the text.[135] The drafters were aware of this potential from the beginning, and U.N. Economic and Social Committee philosophers were consulted. Their opinion was that "[w]here basic human values are concerned, cultural diversity has been exaggerated."[136] The opponents of the universality of the UDHR often overlook the fact the Chinese representative was the vice chairman of the commission. Also, many developing nations did play a role in creating the Declaration with membership on the commission.[137]

Freedom of expression and freedom to information on different sides of the same coin and have been considered to be vitally important since the founding of the United Nations. In the U.N. General Assembly's first session, the assembly passed a resolution calling the "[f]reedom of information a fundamental human right and the touchstone of all the freedoms to which the United Nations is consecrated . . . ."[138] This freedom was included within the UDHR in Article 19, which states, "[e]veryone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[139] The goal of the UDHR is a world where individuals can express themselves how they see fit and have an unobstructed flow of information across.[140] Article 19 seems to do that well, espousing a liberal freedom without any limitations. In fact, only one of the drafts of the UDHR for freedom of speech contained any limitations within the article.[141] While it may appear to be absolute, the UDHR provides for limitations to all rights contained in the Declaration within Article 29. Article 29 purports to limit those rights by stating, "everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements

---

[134] Normand & Zaidi, *supra* note 108, at 194.

[135] *Id.* at 195.

[136] Glendon, *supra* note 109, at 222.

[137] *Id.* at 225.

[138] Calling of an International Conference on Freedom of Information, G.A. Res. 59(I), U.N. GAOR, 1st Sess. (Dec. 14, 1946).

[139] Universal Declaration of Human Rights, G.A. Res. 217A, U.N. GAOR, 3d Sess., 1st plen. mtg., U.N. Doc. A/810 (Dec 12, 1948).

[140] Eide, et al., *supra* note 106, at 278.

[141] Glendon, *supra* note 109, at 271-314. That was what is known as the "Cassin draft" (the second draft). *Id.* The restriction was only to prohibit defamation. *Id.*

of morality, public order and the general welfare in a democratic society."[142] What Article 29 leaves out is any guidance on what meets the requirements of the article versus what would be too stringent a limitation. By the terms of Article 29, a state could have a law restricting speech or any right in the UDHR, as long as the goal was to respect others' freedoms and public order, such as blasphemy restrictions.

B. The International Covenant on Civil and Political Rights

After completion of the UDHR, the Human Rights Commission began to press for a binding covenant on states to enforce the aspirational rights found in the UDHR.[143] The result was the International Covenant on Civil and Political Rights (ICCPR).[144] Currently, there are 167 states parties to the ICCPR, with the United States signing the treaty on 5 Oct 1977, and ratifying the treaty on 8 June 1992.[145]

While the United States finally ratifed the treaty 15 years after signing, the United States submitted reservations, understandings, and declarations (RUDs) to the terms of the treaty, as many other states have done.[146] The only U.S. reservation regarding the freedom of expression is regarding Article 20. The reservation states, "[t]hat article 20 does not authorize or require legislation or other action by the United States that would restrict the right of free speech and association protected by the Constitution and laws of the United States."[147] In other words, the United States will follow the U.S. Constitution and laws, instead of the treaty regarding

---

[142] *Id.* art. 29.

[143] Magnuson, *supra* note 101, at 279.

[144] ICCPR, *supra* note 8.

[145] International Covenant on Civil and Political Rights Status, *available at* http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en (last visited Jan. 13, 2013) [hereinafter ICCPR Status].

[146] *Id.*; *see also* Jack Goldsmith, *The Unexceptional U.S. Human Rights RUDs*, 3 U. St. Thomas L.J. 311 (2005) (arguing that while the U.S. has taken criticism over submitting RUDs to treaties, states submitting RUDs is not unusual, and does not affect the treaty or the U.S.'s commitment to international human rights. The article also demonstrates that liberal democracies tend to take RUDs on human rights treaties, while states that respect human rights less tend not to take any RUDs).

[147] *Id.* There has been some controversy in the idea of states taking RUDs to treaties, and in recent times new challenges to the RUD regime have emerged, especially regarding human rights treaties. *See* Konstantin Korkelia, *New Challenges to the Regime of Reservations under the International Covenant on Civil and Political Rights*, 13 Eur. J. Int'l L. 437 (2002). This article presents a good discussion of the two viewpoints regarding RUDs. One view holds the position that since consent is the governing principle, states have the power to determine the validity of parts of the treaty and may take whatever RUD the state deems appropriate. The other view is that human rights treaties are different, and that there should be a "treaty supervisory organ" that rules on the admissibility of any RUD taken on the treaty. *Id.* at 438. The Human Rights Committee, created by the ICCPR, has taken the position in its General Comment No. 24 that it has the authority to make the determination as to the admissibility of RUDs, and to sever inadmissible reservations. *Id.* This gets to the heart of a potential problem in international law, in that if RUDs were not able to be taken, how many states would ratify the treaty?

how the freedom of expression is able to be restricted. If the Constitution would prohibit restrictions on the freedom of expression and the ICCPR would require them, the U.S. will allow the speech. The United States has a more liberal view of the freedom of expression than most other countries and the ICCPR, and took this reservation as an attempt to safeguard its current and historical interpretation of the First Amendment to the Constitution.[148]

The drafters of the new ICCPR included protections for the freedom of expression in Article 19. Article 19 states:

> 1. Everyone shall have the right to hold opinions without interference.
> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
> 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
> (a) For respect of the rights or reputations of others;
> (b) For the protection of national security or of public order (ordre public), or of public health or morals.[149]

It has been said the text of Article 19 "secures [the] key component of individual liberty, the right to form his or her own opinions free from outside influence and to defend them without fear of external repression."[150] Article 19 allows persons to make and hold opinions without any form of restrictions. This right is absolute; however, the right to seek or impart information may be restricted by the state.[151] Article 19 states the right to freedom of expression carries with it "special duties and responsibilities" that allow states to restrict a person's freedom in certain cases.[152] Inclusion of this provision was controversial.[153] The states that supported inclusion argued speech holds special powers in public opinion, which justifies the inclusion.[154] Those states against the provision, including the United States, argued

---

[148] *See infra* Part IV.A.

[149] ICCPR, *supra* note 8, at art. 19.

[150] Scott N. Carlson & Gregory Grisvold, Practical Guide to the International Covenant on Civil and Political Rights 119 (2003).

[151] ICCPR, *supra* note 8, art. 19.

[152] *Id.*

[153] Magnuson, *supra* note 101, at 280 (citing Marc J. Bossuyt, Guide to the "Travaux Preparatoires" of the International Covenant on Civil and Political Rights 379 (1987)).

[154] *Id.*

all rights also come with duties, and there was no reason to specifically include the responsibility of a speaker.[155]

Speech in the ICCPR did not stop at Article 19; Article 20 also discusses expression, except only in a negative context. Article 20 states that, "1. Any propaganda for war shall be prohibited by law. 2. Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law."[156] Article 20 makes paragraph 3 of Article 19 even clearer. While it specifically prohibits war propaganda without restriction, speech that could be classified as "advocacy of national, racial or religious hatred" must be an incitement to violence or discrimination, without defining any of those terms.[157]

The Human Rights Committee is the body of independent experts established by the ICCPR to monitor compliance with the ICCPR treaty.[158] Further, states parties to the ICCPR are required by the treaty to submit reports every four years on how the state is proceeding with protecting the rights contained within the treaty.[159] In addition to monitoring compliance, the Committee periodically publishes a memorandum with its interpretation of a particular provision of the treaty. These are known as "General Comments," and the Committee has published 34 of them since 1981.[160] Relating to the freedom of expression, the Committee has published General Comments 10, 11, and 34.[161]

General Comment (GC) 10 is the Committee's first interpretation of Article 19. This comment is very brief and does not add much to the understanding of Article 19.[162] GC 11 is the Committee's interpretation of Article 20. This GC is also very brief and does not add to the discussion of what type of speech Article 20 prohibits.[163] However, in 2011 the Committee issued GC 34 which expressly replaced GC 10.[164]

---

[155] *Id.*

[156] ICCPR, *supra* note 8, art. 20.

[157] *Id.*

[158] *Human Rights Committee*, Office of the United Nations High Commissioner for Human Rights (last visited Jan 16, 2013,), http://www2.ohchr.org/english/bodies/hrc/index.htm.

[159] *Id.*

[160] *Id.*

[161] Human Rights Committee, International Covenant on Civil and Political Rights, General Comment No. 10, 19th Sess., CCPR/C/GC/10 (June 29, 1983), Human Rights Committee, International Covenant on Civil and Political Rights, General Comment No. 11, 19th Sess., CCPR/C/GC/11 (Jul. 29, 1983), Human Rights Committee, International Covenant on Civil and Political Rights, General Comment No. 34, 102nd Sess., CCPR/C/GC/34 (Sept. 12, 2011).

[162] Human Rights Committee, International Covenant on Civil and Political Rights, General Comment No. 10, 19th Sess., CCPR/C/GC/10 (June 29, 1983).

[163] Human Rights Committee, International Covenant on Civil and Political Rights, General Comment No. 11, 19th Sess., CCPR/C/GC/11 (July 29, 1983).

[164] Human Rights Committee, International Covenant on Civil and Political Rights, General

In GC 34 the Committee goes through in detail their opinion of what Article 19 means within the ICCPR. GC 34 makes it clear Article 19 and Article 20 work together and complement each other, and speech limited in accordance with Article 20 must also comply with Article 19.[165] The GC lays out that the freedom of expression is essential for any free person and speech is the "foundation stone for every free and democratic society."[166] The Committee believes all forms of speech, whether art, newspapers, verbal or non-verbal, are protected by Article 19. While the comment specifically includes speech that is "deeply offensive" as protected, it immediately turns around and holds that "deeply offensive" speech may be prohibited in accordance with the provisions of Article 19 (3).[167] The limitation in the restrictions available in Article 19 (3) is that the restrictions may not "put in jeopardy the right itself, and that any restrictions must not be overbroad, that the restrictions must be proportional to achieve the aim of restricting the prohibited speech without curtailing any other speech which would be permissible."[168] This appears to be in support of a principle that the exceptions (restrictions on free expression) must not overcome the rule (free expression). The GC makes it clear that the Committee does not believe the ICCPR allows restrictions of the freedom of expression that stem from tradition, religion, or other custom. This includes expressions that convey a lack of respect for certain religions, except as allowed by Article 20.[169] However, the state must be careful not to support one religion in favor of another, as that would not be permissible under the ICCPR.[170]

### C. Hate Speech

One of the theories postulated by the proponents of restricting blasphemous speech, or in support of restricting speech that defames religion, is an attempt to equate it to hate speech.[171] The theory goes that if you can restrict hate speech, then you can restrict blasphemous speech. But what is hate speech? Article 20 of the ICCPR prohibits speech that is considered to be "advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence."[172] But that is an inadequate definition. It does little to tell the states parties what speech they can and cannot restrict. Unfortunately, there is no better definition contained in any legal

---

Comment No. 34, 102nd Sess., CCPR/C/GC/34 at para. 1 (Sept. 12, 2011) [hereinafter GC 34].

[165] *Id.* para. 50.

[166] *Id.* para. 2.

[167] *Id.* paras. 11-12.

[168] *Id.* para. 21.

[169] *Id.* paras. 24 and 48.

[170] *Id.* para. 48.

[171] *See, e.g.*, Osama Siddique & Zahra Hayat, *Unholy Speech and Holy Laws: Blasphemy Laws in Pakistan—Controversial Origins, Design Defects, and Free Speech Implications*, 17 Minn. J. Int'l L. 303 (2008).

[172] ICCPR, *supra* note 8, art. 20.

international law document.[173] The non-governmental organization (NGO) Article 19, a group whose stated mission is to defend freedom of expression,[174] created what they call "The Camden Principles on Freedom of Expression and Equality" in 2009, which contains a definition of hate speech.[175] It defines hate speech as "any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence (hate speech)."[176] This, however, is no different from the ICCPR. The Camden Principles add in Principle 12.1 (i) that "'hatred' and 'hostility' refer to intense and irrational emotions of opprobrium, enmity and detestation towards the target group."[177] It also defines the terms "advocacy" and "incitement," by any statement that may create an "imminent risk of discrimination."[178] So while The Camden Principles do help to clarify what may be hate speech, it is still a broad definition, which could be whatever a state wants it to be. In fact, the definition of hate speech changes over time. One expert relates:

> Traditionally it included any form of expression deemed offensive to any racial, religious, ethnic, or national group. In the 1980s some campus speech codes broadened it to include gender, age, sexual preference, marital status, physical capacity, and other categories. Human Rights Watch defines hate speech as 'any form of expression regarded as offensive to racial, ethnic and religious groups and other discrete minorities, and to women.' Rodney Smolla defines it as a 'generic term that has come to embrace the use of speech attacks based on race, ethnicity, religion and sexual orientation or preference.' Historically, hate speech has been referred to by several terms. In the late 1920s and early 1930s it was known as 'race hate.' Beginning in the 1940s it was generally called 'group libel,' reflecting the specific legal question whether the law of libel should be expanded to cover groups as well as individuals. In the 1980s 'hate speech' and 'racist speech' became the most common terms.[179]

---

[173] *See id.,* Universal Declaration of Human Rights, *supra* note 139, and International Convention on the Elimination of All Forms of Racial Discrimination, 660 U.N.T.S. 195 art. 4, *entered into force* Jan. 4, 1969 (requiring governments to outlaw "all dissemination of ideas based on racial superiority or hatred' as well as 'organizations . . . which promote and incite racial discrimination").

[174] Article 19 Mission, http://www.article19.org/pages/en/mission.html (last visited Mar. 13, 2013).

[175] *The Camden Principles on Freedom of Expression and Equality*, Article 19, (2009) *available at* http://www.article19.org/data/files/medialibrary/1214/Camden-Principles-ENGLISH-web.pdf.

[176] *Id.* principle 12.

[177] *Id.*

[178] *Id.*

[179] Claudia E. Haupt, *Regulating Hate Speech—Damned if you Do and Damned if you Don't: Lessons Learned from Comparing the German and U.S. Approaches*, 23 B.U. Int'l L. J. 299, 304 (2005) (citing Samuel Walker, Hate Speech: The History of an American Controversy 8 (1994)).

Any definition of hate speech necessarily is impacted by the time we are viewing the questioned speech and where we are viewing it. The difficulty in defining the term makes any regulation of it more difficult, but many states around the world currently do restrict hate speech.[180]

While it may be debatable what exactly constitutes hate speech, international law permits its restriction. It is clear in the drafting history of the ICCPR that the delegates were concerned about advocacy of discrimination and racial hatred, and sought to limit it in the draft treaty.[181] This thought continued through the development of the treaty and after the treaty was put into effect. In 1988, the U.N. Commission on Human Rights appointed two Special Rapporteurs on Freedom of Expression to study the right of freedom of expression.[182] The Rapporteurs found that restricting hate speech is completely compatible with the Article 19 right to free expression, since Article 19 carries with it "special duties and responsibilities."[183]

Therefore, while international law clearly provides for limitations to the right of freedom of expression in order to prohibit hate speech, could blasphemous speech meet the vague definition of hate speech and be permissibly restricted? The Human Rights Committee does not take this view. As discussed above, GC 34 indicates that blasphemy cannot be restricted, except in limited circumstances.[184] Even using the definitions in The Camden Principles would not appear to include blasphemy as hate speech.

## IV. BLASPHEMY AND FREEDOM OF EXPRESSION IN DIFFERENT COUNTRIES

Any discussion of blasphemy as a strategic interest of the United States requires a precursor analysis of how U.S. laws are different from Muslim states' laws in this regard. The differences are great. The Muslim states generally put a primacy on their religion and its protection over the right of the individual. This stems from the main beliefs of Islam that there is only one God, the Prophet Mohammad is His

[180] *See, e.g.*, Thomas J. Webb, *Verbal Poison—Criminalizing Hate Speech: A Comparative Analysis and a Proposal for the American System*, 50 Washburn L. J. 445, 446 (2011) (stating that most nations regulate hate speech in order to protect human dignity and minorities).

[181] *See* Stephanie Farrior, *Molding the Matrix: The Historical and Theoretical Foundations of International Law Concerning Hate Speech*, 14 Berkeley J. Int'l. L. 1, 21 (1996).

[182] *Id.* at 88. The Special Rapporteurs' reports are *available at*: Special Rapporteur on the Freedom of Expression, *The Right to Freedom of Opinion and Expression: Final Report*, U.N. Doc. E/CN.4/Sub.2/1992/9 (14 July 1992) (by Mr. Danilo Turk & Mr. Louis Joinet), Special Rapporteur on the Freedom of Expression, *Final Report, Conclusions and Recommendations*, U.N. Doc. E/CN.4/Sub.2/1992/9/Add.1 (14 July 1992) (by Danilo Turk & Louis Joinet).

[183] Farrior, *supra* note 181, at 91.

[184] *See* GC 34, *supra* note 164, para. 48.

final messenger, and the *Quran* is the word of God, and is absolute and irrevocable.[185] These states are often recognized as Islamic states, where the religion and state are inseparable.[186] Below are brief discussions of the blasphemy and freedom of expression laws from the United States, Tunisia, Egypt, and Pakistan. Important to note is that Tunisia and Egypt have recently undergone, and are still undergoing, transformation through what is known as the "Arab Spring."[187]

## A. United States of America

The United States has a very expansive guarantee of the freedom of expression. This right is protected in the First Amendment to the U.S. Constitution.[188] The Supreme Court has upheld few restrictions on the freedom of expression, and generally only upholds those restrictions that are content neutral.[189] This is true regardless how offensive some people may find the speech. The U.S. system protects almost all speech, supporting the principle that the only remedy for bad speech is more speech.[190] "The offensive nature of the speech, far from justifying its prohibition, is precisely why it is entitled to constitutional protection."[191] However, the right to free expression is not absolute.

Two examples of this stem from Supreme Court cases. The Supreme Court, in Brandenburg v. Ohio, stated for speech to be regulated as an incitement it must provoke imminent lawless action and that the lawless action is likely to occur.[192] Also, the Supreme Court laid out another exception to the First Amendment in Chaplinsky

---

[185] Rebecca J. Dobras, *Is the United Nations Endorsing Human Rights Violations? An Analysis of the United Nations' Combating Defamation of Religions Resolutions and Pakistan's Blasphemy Laws*, 37 Ga. J. Int'l & Comp. L. 339, 346 (2009).

[186] *Id.*

[187] *The Arab Spring: A Year of Revolution*, NPR News, Dec. 17, 2011, http://www.npr.org/2011/12/17/143897126/the-arab-spring-a-year-of-revolution [hereinafter The Arab Spring]. The people from both Tunisia and Egypt have overthrown their governments and are in the process of instituting new ones, including drafting and approving new constitutions. *Id.* This will be discussed in more detail in Part III.B and III.C.

[188] U.S. Const. amend. I.

[189] Haupt, *supra* note 179, at 317.

[190] Robert A. Sedler, *An Essay on Freedom of Speech: The United States versus the Rest of the World*, 2006 Mich. St. L. Rev. 377, 383-84 (2006).

[191] *Id.* at 383; *see also* Ronald J. Krotoszynski, Jr., The First Amendment in Cross-Cultural Perspective: A Comparative Legal Analysis of the Freedom of Speech 12-25 (2006) (discussing the different theories behind First Amendment jurisprudence including Justice Holmes' "marketplace of ideas" (the idea that all speech is good and that the truth will win out in the end) or the "public-good-based approach" (the idea that free speech exists to mainly facilitate democracy and that "everything worth saying gets said") that have competed in the case law).

[192] Brandenburg v. Ohio, 395 U.S. 444 (1969).

v. New Hampshire.[193] In Chaplinsky the Court established a narrow exception for speech that can be considered as "fighting words," words which by their very nature "inflict injury or tend to incite an immediate breach of the peace."[194] Thus, while there are restrictions on expression in the United States, the United States has very expansive protections for the freedom of speech.

The United States does not ban speech that is considered blasphemous, unless it meets one of the other exceptions to the First Amendment. While some U.S. states do still have blasphemy laws on the books, they are no longer enforceable.[195] The Supreme Court, in the case Joseph Burstyn, Inc v. Wilson, held blasphemy laws were unenforceable restraints of the freedom of speech contained in the First Amendment.[196] The Court held "[i]t is not the business of government in our nation to suppress real or imagined attacks upon a particular religious doctrine, whether they appear in publications, speeches, or motion pictures."[197] Therefore, it is clear no laws banning blasphemous speech will be enforceable in the United States.

The U.S. national law on the freedom of expression is more expansive than international law; a person in the United States has the ability to say, without worry of sanction, more than what the ICCPR would allow. The ICCPR states speech should be restricted to stop religious or racial hatred, protect national security, or protect public morals.[198] The U.S. domestic law does not permit these types of restrictions, except in very limited circumstances. The U.S. law violates the ICCPR, in this regard, as it is too permissive and allows too much speech.[199] However, as discussed in Part III.B, the United States submitted RUDs when it ratified the ICCPR, and did not ratify the restrictions on free speech in the ICCPR.[200]

### B. Tunisia

In December 2010, a twenty-six year old Tunisian man, an owner of a fruit stand, set off the Arab Spring when he set himself on fire in front of a government building as an act of protest.[201] This act of desperation set off a chain of events not only in his country, but in many other states around North Africa and the Middle

---

[193] Chaplinsky v. New Hampshire, 315 U.S. 568 (1942).

[194] *Id.* at 571-72.

[195] Michael McGough, *Americans Have Cracked Down on Blasphemy Too*, L.A. Times, Sept. 25, 2012, http://articles.latimes.com/2012/sep/25/news/la-ol-obama-blasphemy-islam-20120925. Massachusetts and Pennsylvania still have blasphemy laws in their code. *Id.*

[196] Joseph Burstyn, Inc. v. Wilson, 343 U.S. 495 (1952).

[197] *Id.* at 505.

[198] ICCPR, *supra* note 8, arts. 19-20.

[199] *Id.*

[200] ICCPR Status, *supra* note 145.

[201] *See* The Arab Spring, *supra* note 187.

East, with the effects still being felt today. The protests that followed in Tunisia led to the peaceful ouster of President Zine el Abidine Ben Ali and his government.[202]

The Tunisian people had their first free elections in October 2011 when they elected members for the National Constituent Assembly (NCA). The NCA was tasked with drafting a new constitution because the last constitution (drafted in 1959) was suspended in March 2011.[203] The NCA released the first draft of the new constitution in August 2012.[204] This draft was met with stiff criticism from human rights groups. Both Human Rights Watch and Article 19 both expressed concern the constitution did not do enough to protect free expression and noted the draft criminalized blasphemy.[205] A second draft, released in January 2013, removed the criminalization of blasphemy article, but vague and ambiguous phrasing on free expression remains.[206] The new draft constitution is still undergoing review, and there is hope the protections for the freedom of expression will continue to improve.

After the overthrow of President Ben Ali, the newly elected authorities promised to uphold the freedom of expression both in the constitution and in the laws.[207] In practice, however, the repression of free speech continued. While the Tunisian Penal Code currently does not contain an anti-blasphemy provision, the ruling Ennahdha Movement has promised to "protect the sacred," and to do so has proposed an anti-blasphemy law.[208] This proposed law would be Article 165b in the Tunisia Penal Code.[209] The proposed law would criminalize any "insult, mockery, disdain or physical or moral desecration" of the "sacred values" or symbols.[210] While this proposal has not been made law yet, blasphemy is still being prosecuted in Tunisia. The government has used Article 121(3) of the Tunisia Penal Code to

---

[202] *Id.*

[203] Amnesty Int'l, One Step Forward, Two Steps Back? One year since Tunisia's Landmark Elections 1 (Oct 22, 2012) [hereinafter Amnesty International], *available at* http://www.amnestyusa.org/research/reports/one-step-forward-two-steps-back-one-year-since-tunisia-s-landmark-elections.

[204] Sarah Leah Whitson, *Letter to Members of the Tunisian National Constituent Assembly*, Hum. Rts. Watch, Sept. 13, 2012, http://www.hrw.org/news/2012/09/13/letter-members-tunisian-national-constituent-assembly.

[205] *Id.*; *see also Tunisian Draft Constitution Needs More Work to Protect Freedom of Expression,* Article 19, (Nov. 9, 2012) http://www.article19.org/resources.php/resource/3512/en/tunisa-draft-constitution-needs-more-work-to-protect-freedom-of expression.

[206] *Amnesty Voices Concern Over Tunisia Draft Constitution*, Agence France-Presse, Jan. 12, 2013, http://reliefweb.int/report/tunisia/amnesty-voices-concern-over-tunisia-draft-constitution.

[207] *Id.*

[208] Afef Abrougui, *Free Speech in Tunisia: New Year, Same Fears*, Uncut, Jan. 4, 2013, http://uncut.indexoncensorship.org/2013/01/tunisia-free-speech/.

[209] *Id.*

[210] *Tunisia: Draft Law Amending and Completing Specific Provisions of the Penal Code on the Criminalisation of Offences against Sacred Values*, Article 19, Aug. 2012, *available at* http://www.article19.org/data/files/medialibrary/3411/12-08-16-LA-tunisia.pdf.

criminalize alleged blasphemy.[211] The law prohibits publications that are "liable to cause harm to the public order or public morals."[212] This broad definition has been interpreted by government officials to include alleged blasphemy.

In April 2012, two young Tunisian men were sentenced to seven years in prison for posting cartoons of the Prophet Muhammad naked on Facebook.[213] A spokesman for the Justice Ministry was quoted as saying that the sentence was for a "violation of morality, and disturbing public order."[214] In May 2012, a television station owner, Nabil Karoui, was found guilty and fined 2,400 dinar (approximately $1,500) for airing the critically acclaimed film "Persepolis," which contained an image of Allah.[215] In September 2012, Ayoub Massoudi was sentenced to a suspended four-month term for "undermining the reputation of the army" and "defaming a civil servant" for criticizing the extradition of the former Libyan Prime Minister from Tunisia back to Libya.[216]

While the Arab Spring brought the promise of democratic reforms and new freedoms for the Tunisian people, the reality has been farther from that. The unfortunate reality is people are prosecuted for their speech, especially regarding speech considered to be blasphemous. Part of this stems from some conservative Muslims who want more faith in their public life, versus secularists who want to minimize the role of religion in their public life.[217] Unlike the U.S. Constitution which clearly protects the right to free expression, the draft Tunisian constitution is vague and ambiguous about the protections free expression will receive in the post-Arab Spring Tunisia.

Current Tunisian domestic law is not in compliance with international law. Tunisia ratified the ICCPR in 1969, and is thus bound to meet its requirements.[218] In order to meet their obligations under the ICCPR, Tunisia must clearly define and protect the right of freedom of expression in their new constitution. The use of Article 121(3) and the proposed Article 165b both impermissibly curtail the right

---

[211] *Id.*

[212] *Id.*

[213] Reuters, *Tunisia Jails 2 for Posting Cartoons on Facebook*, N. Y. Times, Apr. 5, 2012, http://www.nytimes.com/2012/04/06/world/africa/tunisia-jails-2-for-facebook-cartoons-of-prophet.html?_r=0.

[214] *Id.*

[215] *Tunisian Court Levies Fine on Persepolis Cinema Owner*, The Telegraph, May 3, 2012, http://www.telegraph.co.uk/news/worldnews/africaandindianocean/tunisia/9242927/Tunisian-court-levies-fine-on-Persepolis-cinema-owner.html.

[216] *See* Amnesty Int'l, *supra* note 203, at 27.

[217] Reuters, *supra* note 213.

[218] ICCPR Status, *supra* note 145.

to free speech as guaranteed by the ICCPR.[219] The restrictions on speech in Tunisia do not meet the exceptions laid out by Article 19 or 20 of the ICCPR.

## C. Egypt

Like Tunisia, the Egyptian people were swept up in the tide of the Arab Spring and overthrew their government, led by President Hosni Mubarak, in February 2011.[220] Once the government was overthrown, the military suspended the constitution.[221] Elections were held in November 2011, and a new president was elected, Muhammad Morsi.[222]

While the constitution had provisions that protected the right of freedom of expression, President Mubarak's regime suppressed most rights, with the constitution's terms meaning little.[223] On December 26, 2012, President Morsi signed a decree that put into effect the recently voter-approved new constitution.[224] This new constitution has already been heavily criticized for its apparent lack of protection for fundamental human rights.[225] Freedom of expression, while protected in the constitution, is limited in several ways. The new constitution bans blasphemy and forms of "insult," as well as only permitting the "divine" or "monotheistic" religions.[226] Human Rights Watch takes the position that the constitution fails to sufficiently protect the freedom of expression by vaguely defining what the limitations are to speech and when the state is allowed to limit it.[227] Some members of the Egyptian media argue this new constitution has worse protections for the media than it had during Mubarak's regime. They argue if an individual reporter makes a mistake, then the government can shutdown the entire publication.[228] In addition to the constitution, there are limits on freedom of expression found in the penal law.

---

[219] *See also* Tunisia: Draft Law Amending and Completing Specific Provisions of the Penal Code on the Criminalisation of Offences against Sacred Values, *supra* note 210.

[220] The Arab Spring: *A Year of Revolution*, *supra* note 187.

[221] *Egypt: Protecting Freedom of Expression and Freedom of Information in the New Constitution,* Article 19, 9 (2012), *available at* http://www.article19.org/data/files/medialibrary/3092/12-05-09-LA-egypt.pdf.

[222] Salma Abdelaziz, *Morsy Signs Egypt's Constitution into Law*, CNN.com, Dec. 26, 2012, http://www.cnn.com/2012/12/25/world/africa/egypt-constitution/index.html.

[223] *Egypt: Protecting Freedom of Expression and Freedom of Information in the New Constitution, supra* note 221.

[224] Abdelaziz, *supra* note 222.

[225] Isobel Coleman, *The Explosive Debate over Egypt's new Constitution*, The Atlantic, Dec. 5, 2012, http://www.theatlantic.com/international/archive/2012/12/the-explosive-debate-over-egypts-new-constitution/265931.

[226] *Id.*

[227] *Egypt: New Constitution Mixed on Support of Rights*, Hum. Rts. Watch, Nov. 30, 2012, http://www.hrw.org/news/2012/11/29/egypt-new-constitution-mixed-support-rights.

[228] Mosireen, *Egypt's Draft Constitution in Focus: Freedom of Expression*, Jadaliyya, Dec. 20, 2012,

The Egyptian Penal Code, while not having a law that specifically prohibits blasphemy, does contain Article 98(f) which prohibits using religion to "promote or advocate extremist ideologies, ignite strife, degrade any of the heavenly religions, or harm national unity or social peace."[229] The Egyptian law also contains the "doctrine of *hisba* which entitles any Muslim to take legal action against anyone he considers harmful to Islam."[230] This doctrine has given some Islamic extremists the ability to harass scholars and others seen as insulting Islam, including members of other sects of Islam, Judaism, or Christianity.[231]

During the short presidency of Mr. Morsi, the prosecutions for insulting the president or the judiciary have increased.[232] Bassem Youssef, a television comedian, is being investigated for insulting President Morsi and other conservative Islamists, with the complainants stating his skits amounted to a "sharp attack on the person of the president," or "sarcasm against the president."[233] An Egyptian court recently sentenced to death seven Coptic Egyptians living abroad after trial in absentia for their connection to the film "Innocence of Muslims."[234]

The new Egyptian constitution and current criminal investigations and prosecutions put great limits on the freedom of expression. The constitution gives too much power to the state, almost to the point where free expression exists in name only. The new Egyptian constitution, filled with limitations on free expression, is hardly protective of free expression. This constitution arguably violates Egypt's requirements under the ICCPR, which Egypt ratified in 1982, by imposing restrictions that fall outside of the limitations allowed in Articles 19 and 20 of the ICCPR.[235]

### D. Pakistan

Pakistan's blasphemy laws have often made for tragic international headlines after another incident of oppression of minority groups.[236] While Pakistan has laws

---

http://www.jadaliyya.com/pages/index/9139/egypts-draft-constitution-in-focus_freedom-of-expr.

[229] Marshall & Shea, *supra* note 14, at 67.

[230] *Id.* at 62 (emphasis in original).

[231] *Id.*

[232] *Egypt: New Constitution Mixed on Support of Rights*, *supra* note 227.

[233] Mayy El Sheikh, *Egypt: Prosecutor Opens Criminal Investigation Against Comedian Accused of Insulting the President*, N. Y. Times, Jan. 1, 2013, http://www.nytimes.com/2013/01/02/world/middleeast/comedian-accused-of-insulting-egyption-president-to-be-investigated.html?ref=middleeast&_r=0.

[234] Mohamed Fadel Fahmy, *Egyptian Court Orders Death Sentences over Anti-Islam Film*, CNN.com, Nov. 29, 2012, http://cnn.com/2012/11/28/world/meast/Egypt-anti-islam-film/index.html?hpt=wo_c2.

[235] ICCPR Status, *supra* note 145.

[236] *See* Siddique & Hayat, *supra* note 171; *see* Rebecca J. Dobras, *Is the United Nations Endorsing Human Rights Violations? An Analysis of the United Nations' Combating Defamation of Religions*

prohibiting blasphemous speech, their constitution purports to protect the right to free expression.[237] However, a quick review of Article 19 of the constitution reveals there are several provisions that allow the state to limit the right to free speech. Speech can be limited by "reasonable restrictions imposed by law in the interest of the glory of Islam" or in national defense, or as part of "friendly relations" with foreign powers, or for public order.[238] This is in stark contrast to the U.S. Constitution which contains no limitations on the right to free speech.

The Pakistani courts tend to view free speech on a case-by-case approach in order to best gauge the "reasonableness" of the state's restrictions and to best balance the state's interests.[239] The courts have case law that has supported freedom of speech as it concerns the press, and struck down attempted regulation of the press.[240] In contrast to this limited case law that may be an attempt to support the freedom of expression, Pakistan has consistently been named one of the world's deadliest places for reporters, with reporters threatened until they leave cities, and websites to news organizations routinely blocked.[241]

The Pakistan Penal Code contains strict blasphemy provisions in order to punish people for defaming Islam.[242] These blasphemy laws protect Islam and the Prophet Muhammad from criticism or any type of defiling of his name or Islam's holy books.[243] The punishment for blasphemy can be up to a maximum of life in prison or death.[244] These statutes have routinely been arbitrarily enforced to repress minorities, such as the Ahmadis, a minority religious sect.[245] A senior researcher at Human Rights Watch notes that "Pakistan has set the standard for intolerance when it comes to misusing blasphemy laws . . . ."[246]

---

*Resolutions and Pakistan's Blasphemy Laws*, 37 Ga. J. Int'l & Comp. L. 339 (2009).

[237] Pakistan Const. art. 19 (1973) ("Every citizen shall have the right to freedom of speech and expression, and there shall be freedom of the press, subject to any reasonable restrictions imposed by law in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of Court, commission of or incitement to an offence").

[238] *Id.*

[239] Siddique & Hayat, *supra* note 171, at 370-71.

[240] *Id.*

[241] Malik Siraj Akbar, *Pakistan's Eroding Space for Free Expression*, Huffington Post, Aug. 9, 2012, http://www.huffingtonpost.com/malik-siraj-akbar/pakistan-press-freedom_b_1735806.html.

[242] Pak. Penal Code §§ 295-98 (1860), *available at* http://www.refworld.org/docid/485231942.html.

[243] *Id.*

[244] *Id.*

[245] Dobras, *supra* note 236, at 343.

[246] *Pakistan: Drop Blasphemy Charges Against 17-Year-Old*, Hum. Rts. Watch, Feb. 2, 2011, http://www.hrw.org/news/2011/02/02/pakistan-drop-blasphemy-charges-against-17-year-old (discussing a case where a seventeen-year-old was arrested for blasphemy for allegedly including derogatory remarks about the Prophet Muhammad on an exam. The police stated that they cannot disclose any

The evidence used to determine if someone committed a blasphemous act is up to the subjective biases and opinions of the state official.[247] No further evidence of blasphemy is required; the government will usually accept any complaint of blasphemy and not conduct an investigation. The complaint is often sufficient to convict someone of blasphemy, without any consideration of the complainant's motivations.[248] There have been occasions of "religious vigilantism" occurring in Pakistan, where groups of extremists have attacked and killed alleged blasphemers.[249] However, those people convicted of blasphemy at trial often have their convictions overturned by the appellate courts.[250] And while the death penalty is an authorized punishment, and several people are on death row for blasphemy, no one has ever been executed in Pakistan for blasphemy.[251]

Pakistan's view of free speech is much different from that of the United States. With the numerous exceptions to their constitutional protections of free speech, clearly a person in Pakistan has less freedom of speech than in the United States. Pakistan's laws on freedom of speech also do not hold up against international law. Pakistan signed and ratified the ICCPR, and as such must meet those terms, which provide far more protections for the freedom of expression than Pakistani law allows.[252] Pakistan's blasphemy laws do not meet the requirements for allowable restrictions on speech found in Articles 19 and 20 of the ICCPR.

## V. DOES THE UNITED STATES' APPROACH TO FREE EXPRESSION PROMOTION ADVANCE ITS FOREIGN POLICY INTERESTS?

The United States' approach to free speech is more than just an interpretation of U.S. and international law. The United States advocacy of the freedom of expression has effects not just on international law, but in non-legal areas, such as global stability and security. This is especially focused in the area of blasphemy and the defamation of religions, as these topics implicate both international law and the political decisions that are made as the United States strives for global security and stability.

---

details of the incident because to do so would be blasphemy).

[247] Dobras, *supra* note 236, at 357 (citing *Persecuted Minorities and Writers in Pakistan* Hum. Rts. Watch (1993), *available at* http://www.hrw.org/legacy/reports/1993/pakistan/).

[248] *Id.*

[249] Dobras, *supra* note 236, at 344.

[250] Siddique & Hayat, *supra* note 171, at 374.

[251] *See id.*; *Pakistan's Blasphemy Laws Still Claim Many Victims*, CatholicCulture.org, Nov. 21, 2012, http://www.catholicculture.org/news/headlines/index.cfm?storyid=16326.

[252] ICCPR Status, *supra* note 145. Pakistan took reservations to most provisions of the treaty, to which many nations around the world objected to as incompatible with the treaty. *Id. See also supra* Part III.B.

A. U.S. Policy on the Anti-Defamation Proposals

As discussed in Part II.D, the Organization of Islamic Cooperation (OIC) has pushed for U.N. resolutions that called for limits on speech that was blasphemous or defamed religions. These resolutions were passed by the Human Rights Committee and General Assembly for years. However, in 2011, the language softened and only spoke of combating intolerance or discrimination because of religion or belief. This resolution was adopted by the Human Rights Committee in 2011, and the next year by the General Assembly.[253]

The United States has been against every defamation of religion resolution proposed by states on behalf of the OIC. The United States has held this position since the first defamation of religion resolution was drafted by Pakistan in 1999, and been supported in arguing against these resolutions by most western countries.[254] The United States and many Western states argue these resolutions illegally and improperly restrict the freedom of expression in a way inconsistent with international law.[255] Secretary of State Hillary Rodham Clinton eloquently stated the U.S. position during a speech she gave in 2009:

> Now, some claim that the United Nations can best protect the freedom of religion by adopting what is called "anti-defamation" policy that would restrict the freedom of expression and the freedom of religion. I obviously, strongly disagree. An individual's ability to practice their religion should have no bearing on others [sic] individuals' freedom of speech. The protection of speech about religion is particularly important since persons of different faiths will inevitably hold divergent views on religious questions. And these differences should be met with tolerance, not suppression of discourse. And the United States will stand against the idea of defamation of religion in the United Nations General Assembly and the Human Rights Council.[256]

While the early anti-defamation of religion resolutions passed by landslide margins, each time thereafter the "no" votes gained traction, though the resolutions still passed by a majority vote.[257] In March 2010, after the Human Rights Council passed what ended up being the last (for now) resolution on defamation of religion, the U.S. ambassador to the Council, Eileen Donahoe, summarized the U.S. position

[253] G.A. Res. 66/167, U.N. Doc. A/RES/66/167 (Mar. 27, 2012).

[254] *See id.*

[255] *See id.*

[256] Secretary of State Hillary Rodham Clinton, Remarks Upon Receipt of the Roosevelt Institute's Four Freedoms Award at the Roosevelt Institute's Four Freedoms Medals Gala Dinner (Sept. 11, 2009), *available at* http://www.state.gov/secretary/20092013clinton/rm/2009a/09/129164.htm.

[257] *See* Blitt, *supra* note 76, at 350.

on the resolution when she said, "[W]e cannot agree that prohibiting speech is the way to promote tolerance, because we continue to see the 'defamation of religions' concept used to justify censorship, criminalization, and in some cases violent assaults and deaths of political, racial, and religious minorities around the world."[258]

While the United States may have been against resolutions containing language prohibiting the defamation of religion, the United States supported U.N. Human Rights Council Resolution 16/18 on combating intolerance.[259] The opponents of the defamation of religion resolutions were able to delete any mention of defamation in the resolution, and as such, many states supported Resolution 16/18 that had been against the prior resolutions.

Resolution 16/18 did not end the debate about defamation of religion though. Resolution 16/18 enabled the United States to support it and allowed the United States to claim that the time of putting religious sensitivities of some people over freedom of expression for all was over.[260] The United States also believed that Resolution 16/18 moved the debate in the right direction toward a global discussion on intolerance, discrimination, and violence against persons based on religion or belief.[261] However, the language used in the resolution also allowed the OIC to claim that the resolution was nothing more than the "exploring [of an] alternative approach."[262] These differing viewpoints on the meaning and finality of the "death" of the defamation resolutions signal the fight against limiting free expression is not over. The OIC Charter still lists the fight against the defamation of Islam as one of the organizations basic objectives.[263] The Secretary-General of the OIC was quoted after the passing of Resolution 16/18 as saying that the "perception that supporting [defamation of religion] would throttle one's right to freedom [of] expression is only a myth."[264]

---

[258] *UNHRC Votes by Narrower Margin to Condemn "Defamation of Religion,"* Religion & L. Consortium, Mar. 2010, *available at* http://www.religlaw.org/index.php?blurb_id=805&page_id=25.

[259] Blitt, *supra* note 76, at 350.

[260] *See id.*

[261] Press Release, U.S. Department of State, Adoption of Resolution at Human Rights Council Combating Discrimination and Violence (Mar. 24, 2011), *available at* http://www.state.gov/secretary/20092013clinton/rm/2011/03/159095.htm.

[262] Blitt, *supra* note 76, at 350.

[263] *OIC Charter ¶ 12*, Org. of Islamic Cooperation, http://www.oic-oci.org/page_detail.asp?p_id=53 (last visited Jan. 24, 2013). Paragraph 12 of the OIC Charter states, "To protect and defend the true image of Islam, to combat defamation of Islam and encourage dialogue among civilisations [sic] and religions." *Id.*

[264] Blitt, *supra* note 76, at 362.

With the recent alleged blasphemous acts occurring world-wide,[265] the OIC states have begun pushing for new resolutions with the language reverting back to the old way to attempt to prohibit language that defames religion, especially Islam. These calls have come from both Egypt and Yemen at the U.N., with both countries' presidents demanding limitations on speech that insults religion.[266] What remains to be seen is how the international community will respond; whether the consensus that built up around Resolution 16/18 will stand, or whether the renewed calls for limitation on speech will attract enough support.

B. Does the U.S. Policy Make Sense?

The United States' strident opposition to any resolution condemning or prohibiting blasphemy or the defamation of religion makes sense. Being supportive of expanded human rights will help lead to freedom and justice around the world. Further restrictions on speech will not make the world a better place.

Limiting freedom of expression with restrictions against blasphemy and defamation of religion does not meet the standards of international law. The ICCPR limits speech in Article 19 (3) only when they are "provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals."[267] GC 34 specifically addresses the issue of blasphemy. It holds that no restriction on speech for purely religious reasons can stand in accordance with the terms of Article 19, stating, "[p]rohibitions of displays of lack of respect for a religion or other belief system, including blasphemy laws, are incompatible with the Covenant . . . ."[268]

The other avenue for restricting speech given by the ICCPR is Article 20, which prohibits speech that is advocating "religious hatred that constitutes incitement to discrimination, hostility or violence . . . ."[269] Unfortunately, GC 11 on Article 20, does not help interpret this restriction on speech. A plain reading of the provision appears to prohibit a restriction on expression for the purpose of preventing blasphemy or the defamation of a religion as it is not necessarily advocating any religious hatred. Of course, this changes if the speaker is directly inciting his audience to violence, hostility or discrimination. But this type of speech is more than the simple blasphemy the OIC is attempting to prohibit in the U.N. resolutions. This direct advocacy to violence would even be prohibited under U.S. law.[270] The proponents

---

[265] *See supra* Part II.C.

[266] *See* Neil MacFarquhar, *At U.N., Egypt and Yemen Urge Curbs on Free Speech*, N. Y. Times, Sept. 26, 2012, http://www.nytimes.com/2012/09/27/world/united-nation-general-assembly.html.

[267] *See* ICCPR, *supra* note 8, art. 19.

[268] *See* GC 34, *supra* note 161, para. 48.

[269] *See* ICCPR, *supra* note 8, art. 20.

[270] *See*, *supra* Part IV.A.

of the anti-defamation of religion resolutions and state blasphemy laws (namely the OIC), generally use Article 20 as their means of justifying their laws and the resolution.[271] However, it is generally agreed this would be a redefinition of the law as currently understood internationally.[272] In 2001, the freedom of expression special rapporteurs for the U.N., the Organization of American States, and Organization for Security and Cooperation in Europe jointly issued a statement which argued "no one should be penalized for the dissemination of 'hate speech' unless it has been shown they did so with the intention of inciting discrimination, hostility, or violence."[273]

Democracy is fundamentally about freedom. Human rights, both internationally and nationally, should be about protecting and expanding human freedoms. Blasphemy laws are meant to curtail freedom and opposing ideas. The laws are not used for some higher purpose, but often for the maintenance of the status quo, to keep a side in power by suppressing any other viewpoint and preventing a discussion on other ideas from beginning.[274] The laws that are currently in existence, such as the one in Pakistan, are extremely prone to abuse, often used to suppress minorities within the country.[275]

Proponents of restrictions of speech for blasphemy sometimes argue religion deserves the same protections race receives.[276] However, there is a problem with that comparison. Religion is inherently personal. It is not the same as a person's race. "A person's race is immutable, while religion is a belief that individuals are free to choose or change . . . ."[277] Attempts to equate the two miss the point and are wrong. While criticizing a race infers criticism of a person of that race, criticism of a belief does not.[278] Religions or beliefs do not deserve the same protections that race receives.[279]

The U.S. policy decision to fight the defamation of religions resolutions is correct also because of the vagueness and one-sidedness of the resolutions. The resolutions are written so vaguely it is impossible to know precisely what is being

---

[271] *See* Leonard A. Leo, Felice D. Gaer & Elizabeth K. Cassidy, *Protecting Religions from "Defamation": A Threat to Universal Human Rights Standards*, 34 HARV. J.L. & PUB. POL'Y 769, 775 (2011).

[272] *See id.*

[273] *See id.*

[274] *See id.*

[275] *See supra* Part IV.D.

[276] *See* Courtney C. Radsch, *Why a Global Blasphemy Law is the Wrong Response to Islamaphobia*, HUFFINGTON POST, Oct. 10, 2012, http://www.huffingtonpost.com/Courtney-c-radsch/global-blasphemy-law-wrong-response-to-islamaphobia_b_1920109.html.

[277] *Id.*

[278] *See id.*

[279] *See id.*

limited. Proponents use the phrase "defamation of religion," without any discussion of what that phrase means.[280] Roy W. Brown of the International Humanist and Ethical Union stated it well when he said the following in a letter to the Human Rights Council:

> And how are we to define defamation? Are we no longer to be permitted to condemn misogyny, homophobia, or calls to kill—if they are made in the name of religion? Are we obliged to respect religious practices that we find offensive? Is lack of respect for such practices to be considered a crime? Are ideas, are religions now to be accorded human rights? Surely, when religion invades the public domain it becomes an ideology like any other, and must be open to criticism as such. To deny the claims of religion is neither defamation nor blasphemy.[281]

If the United States supported these measures and supported them becoming international law, would the U.S. then be required to outlaw atheists? Could a person in the United States be allowed to stand up and shout "There is no God," to whoever will listen? Arguably that simple statement is blasphemy and defaming all religions that believe in God and the United States would be required to silence the atheist. This hypothetical may be said to be ludicrous from some supporters of anti-blasphemy resolutions, but it is taking the idea behind the resolutions to its logical extreme. Any thoughts beside what you (the supporter) have are blasphemy and thereby defaming your religion, and needs to be outlawed.

### C. Should There be Limits on What Can be Posted in One Country but Broadcast Internationally?

As traditions against blasphemy are usually cultural and distinct to specific states, one potential solution would be to regulate the speech that emanates from a state. This would have the effect of allowing states like the United States, with its liberal allowances for freedom of expression, to maintain their freedoms, and allow states like Pakistan, with strict blasphemy laws, to not have their laws violated by what is produced in the United States. This solution though, is not workable in our modern technological world. The Internet cannot be limited in that manner without draconian restrictions.

The Internet is an amazing instrument for communication, research, and study all across the world. It has also become, unfortunately, an amazing vehicle to distribute messages of hate.[282] Hate speech and cyber bullying have affected lives

---

[280] *See* Resolutions, *supra* note 83, and *supra* Part II.E.

[281] Statement of Roy W. Brown to Human Rights Council, Int'l Humanist & Ethical Union (Mar. 29, 2007), *available at* http://iheu.org/how-islamic-states-dominate-un-human-rights-council/.

[282] *See* LaShel Shaw, *Hate Speech in Cyberspace: Bitterness without Boundaries*, 25 Notre Dame

all across the world.[283] The U.N. Secretary General has called the use of the Internet to spread hate an important challenge arisen from modern technology.[284]

In order to limit speech to the state of the speaker, you would have to limit the Internet in ways that it has never been limited before. Today, if someone in the United States posted a blasphemous video onto YouTube, that video is viewable by people all across the world, whether the poster intended it to be viewed by people in Pakistan or not.[285] How is the video poster to know it violates some law in Pakistan, on the other side of the world? Should he be liable for that, even though he only intended his family to view the video in a nearby U.S. state?

Blasphemous speech, as discussed in Part II.A, varies by religion. The things/people/items that one religion holds sacred can be very different, and perhaps unexpectedly so, to someone not of that religion. If a group were to call blasphemy hate speech, then what is hate speech? Social and historical context is extremely important in determining what hate speech is.[286] Hateful speech can be different things to different people. "And if you ask what words are likely to be provocative . . . what are likely to be their fighting words, the answer is anything and everything . . . every idea is an incitement to somebody . . . ."[287] It is difficult to put regulations on the Internet on speech that speakers do not, or cannot, know is hateful.

The Internet is transnational by its very nature. Information online exists in some ways "everywhere, nowhere in particular, and only on the Net," and yet can affect people everywhere.[288] In order to make workable a limitation on speech to keep what is spoken in your state in your state, the very nature of the Internet would have to change. Content monitors (censors) would be needed in every state on every ISP to review content before it was posted for wide dissemination. The scale of this project would be immense. Consider that currently over 48 hours of video is uploaded to YouTube every minute from hundreds of millions of users around the world.[289] And this is only one website. The solution is just not workable

---

J.L. Ethics & Pub. Pol'y 279 (2011).

[283] *See id.* at 281.

[284] The Secretary-General, *Preliminary Report of the Secretary-General on Globalization and its Impact on the Full Enjoyment of all Human Rights*, 26-28, U.N. Doc A/55/342 (Aug. 31, 2000).

[285] Shaw, *supra* note 282.

[286] Alexander Tsesis, *Dignity and Speech: The Regulation of Hate Speech in a Democracy*, 44 Wake Forest L. Rev. 497 (2009).

[287] Stanley Fish, There's No Such Thing as Free Speech: And It's a Good Thing Too 106 (1994).

[288] Davis R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 Stan. L. Rev. 1367, 1375 (1996).

[289] About YouTube, Youtube.com, http://www.youtube.com/t/faq (last visited Mar. 13, 2013).

with the Internet and modern telecommunication technology if there is any desire to keep the Internet an open market place of ideas.[290]

D. Would a Different Approach to Free Expression Better Serve U.S. National Security?

The United States should not change its approach to advocating for international freedom of expression. Blasphemous speech does create instability and does present a security risk for the United States.[291] After the "Innocence of Muslims" went viral and the riots began, U.S. agencies warned "[t]he risk of violence could increase both at home and abroad as the film continues to gain attention," putting at risk U.S. interests both at home and abroad.[292] The minimal gain in security the United States would see as a result of changing its law and policy on freedom of expression would not be enough to justify the dramatic changes. The United States would need to override its entire jurisprudential history on the First Amendment, as well as both its and the international community's understanding of international law, in order to prevent blasphemy.[293] One must imagine this radical shift, probably requiring a Constitutional amendment, would throw American society into upheavals. If the United States does not want to go that far, a simple change of foreign policy will not work. If the United States changes to advocating for reduced freedom of expression abroad, but does not curtail the freedom at home, the blasphemous speech will still emanate from the United States, and still cause instability and anger directed at the United States.

It is questionable whether eliminating speech considered blasphemous or defaming Islam emanating from the United States would have any effect on Islamic terrorists. The Islamic terrorists' hatred of the west, and the United States, comes from much more than what westerners say about Islam. This hatred goes back over 100 years to the colonial oppression by the western nations of the Middle Eastern nations.[294] From the early 1900s when the European powers created the nations of the Middle East for their own profit, to the Cold War when the United States and the Soviet Union "fought over the Middle East nations like children over toys," Middle East resentment has grown.[295] During the Cold War, the United States supported

---

[290] *But see Internet Censorship in China*, N. Y. Times, Dec. 28, 2012, http://topics.nytimes.com/topics/news/international/countriesandterritories/china/internet_censorship/index.html (stating that Chinese government computers screen all incoming data and compare it to banned keyword lists and web sites, and then block them).

[291] *See U.S. Warns of Rising Threat of Violence Amid Outrage Over Anti-Islam Video*, CNN.com, Sept 14. 2012, http://www.cnn.com/2012/09/13/world/meast/embassy-attacks-main/index.html.

[292] *Id.*

[293] *See supra* Part IV.A.

[294] William O. Beeman, *Why Middle Eastern Terrorists Hate the United States* (2001), *available at* https://www.brown.edu/Administration/News_Bureau/2001-02/01-025.html.

[295] *Id.*

many despotic, tyrannical rulers in the Middle East; each of whom oppressed their people. This has been cited as a primary cause of Islamic terrorists' desires to target the United States.[296] With a reduction in the importance of blasphemy, the need to adjust the U.S. security policy based on it is reduced.

Islamic political radicals' main fear was identified in a 2006 Gallup survey as American occupation/domination, and the threat thereby to Islam.[297] This in turns leads directly into what has been called the biggest geopolitical force causing Islamic extremism and terrorism, the U.S. military presence in the region and the Palestinian/Israeli conflict.[298] The threat modernity and globalization pose, at least in the minds of the Islamic extremist, is another driving factor in the hatred of the west. This cultural dilemma facing the Middle East causes tensions that result in terrorism. Extremists refer to the West's military presence as modern day crusaders attempting to stamp out Islam and their culture in order to maintain power.[299]

The root causes of the Islamic terrorists' hatred towards the United States and the west stem from more than the west's depictions of Islam. However, from the reaction in the Middle East, it is clear these "blasphemous" actions do throw fuel on the fire. But how much? Jessica Stern, a member of the Hoover Institution Task Force on National Security and Law, disputes some of the commonly held myths, as she puts it, regarding terrorists.[300] One of these myths is terrorists groups are made up of religious zealots. Evidence the Saudi Interior Ministry gained from thousands of interviews of terrorists in custody uncovered that the majority had only a limited understanding of Islam, and one-quarter had criminal histories.[301] Another stated myth is terrorists are strongly motivated by their cause. Research indicates the opposite. In fact, the reasons people join terrorist organizations are extremely varied. This leads to short lived terrorists groups, with ones that survive having a more flexible ideology to support the varied ideology of their recruits. An exception is al Qaeda, which is a disciplined group, but one whose goals shift constantly.[302]

Terror groups may gain new members through anger towards blasphemy by the west, and there could follow a rise in terrorist activities directed towards U.S. interests. However, studies have demonstrated there is no one path or recruitment

---

[296] Young, *supra* note 39, at 11.

[297] *Id.* at 10.

[298] *Id.* at 14. The author specifically cites to the Iraq conflict and insurgency as the cause. This can logically be extended to the U.S. military presence in the region, to include the conflict in Afghanistan against the Taliban.

[299] *Id.* at 17.

[300] Jessica Stern, *5 Myths About Who Becomes a Terrorist*, Wash. Post, Jan. 10, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/01/08/AR2010010803585.html.

[301] *Id.*

[302] *Id.*

pitch that is successful to persuading people to join these groups.[303] While U.S. agencies do fear these acts could be used to exploit anger and obtain new members, it does not appear blasphemy will be a driving force in recruitment.[304] The reasons terrorist groups target the United States are sufficiently distinct from the U.S. free speech policy that there is little evidence to support any assertion that modification of that policy would affect the security of the United States.

## VI. CONCLUSION

Blasphemy by the west towards Islam has contributed to global unrest and instability over the last several years, and will continue to in the future. These acts by individuals, often in the United States exercising their constitutionally protected right to free speech, have resulted in national security threats to the United States and its interests around the world. However, the instability created in the Middle East and North Africa, while causing national security concerns for the United States, is not always bad. The Arab Spring is a good example of this. While it was brought on by decades of oppression, it was spurred on and organized by Internet social media sites like Twitter and Facebook.[305] The power of the Internet and the free speech that it is able to provide can be a powerful force for good across the world.

Even with international law being clear on the matter, this has not stopped, nor will it stop, the OIC from advocating for limiting expression in this manner. Even with Resolution 16/18[306] stepping away from the anti-defamation language, the OIC states have already indicated they will be pursuing an anti-defamation resolution again. President Mohamed Morsi of Egypt, in a speech to the U.N. General Assembly, stated:

> [w]e expect from others, as they expect from us, that they respect our cultural specifics and religious references, and not seek to impose concepts or cultures that are unacceptable to us . . . Insults against the prophet of Islam, Muhammad, are not acceptable. We will not allow anyone to do this by word or by deed.[307]

These words unmistakably indicate the intent of Egypt to press for restrictions on speech similar to the past anti-defamation resolutions.

---

[303] Sara Daly & Scott Gerwehr, *Al-Qaida: Terrorist Selection and Recruitment,* Rand Corp. (2006), *available at* http://www.rand.org/pubs/reprints/RP1214.html.

[304] *Id.*

[305] *See* Carol Huang, *Facebook and Twitter Key to Arab Spring Uprisings: Report*, The Nat'l, June 6, 2011, http://openlab.citytech.cuny.edu/designprocess/files/2012/08/TheNational_FacebookandTwitterKeytoArabSpringUprising.pdf.

[306] Resolution 16/18, *supra* note 87.

[307] MacFarquhar, *supra* note 266.

Even with the clear mandate by international law, blasphemy is still banned in many Islamic countries, as shown in Part IV. This is despite these nations being signatories to the ICCPR.[308] Blasphemy restrictions are alive and well, and they do not appear to be going anywhere in the near future. These countries' actions and words indicate they will continue to advocate for a limitation to the basic human right of freedom of expression for the rest of the world. Nations of the world need to be vigilant, and continue to support the expansion of the freedom of expression.

The U.S. foreign policy on freedom of speech is to advocate for speech with very few limitations, just like U.S. domestic law provides.[309] President Obama eloquently defended the U.S. view of free speech in front of the U.N. General Assembly, and made it clear even if a state does not have quite the expansive view the United States has, there is "no speech that justifies mindless violence."[310] This

[308] *See* Blasphemy Laws in Different Countries, *supra* Part IV.

[309] *See supra* Part II.D.

[310] *Obama's Speech to the United Nations General Assembly—Text*, N. Y. Times, Sept. 25, 2012, http://www.nytimes.com/2012/09/26/world/obamas-speech-to-the-united-nations-general-assembly-text.html?r=0. President Obama stated the U.S. position on free speech as:

> I know there are some who ask why we don't just ban such a video. And the answer is enshrined in our laws: Our Constitution protects the right to practice free speech.
>
> Here in the United States, countless publications provoke offense. Like me, the majority of Americans are Christian, and yet we do not ban blasphemy against our most sacred beliefs. As President of our country and Commander-in-Chief of our military, I accept that people are going to call me awful things every day—(laughter)—and I will always defend their right to do so.
>
> Americans have fought and died around the globe to protect the right of all people to express their views, even views that we profoundly disagree with. We do not do so because we support hateful speech, but because our founders understood that without such protections, the capacity of each individual to express their own views and practice their own faith may be threatened. We do so because in a diverse society, efforts to restrict speech can quickly become a tool to silence critics and oppress minorities.
>
> We do so because given the power of faith in our lives, and the passion that religious differences can inflame, the strongest weapon against hateful speech is not repression; it is more speech—the voices of tolerance that rally against bigotry and blasphemy, and lift up the values of understanding and mutual respect.
>
> Now, I know that not all countries in this body share this particular understanding of the protection of free speech. We recognize that. But in 2012, at a time when anyone with a cell phone can spread offensive views around the world with the click of a button, the notion that we can control the flow of information is obsolete. The question, then, is how do we respond? And on this we must agree: There is no speech that justifies mindless violence. There are no words that excuse the killing of innocents. There's no video that justifies an attack on an embassy. There's no slander that provides an excuse for people to burn a restaurant in Lebanon, or destroy a school in Tunis, or cause death and destruction in Pakistan. In this modern

liberal policy position could create new terrorists when people hear speech coming from the United States they find blasphemous. This is a risk the United States must take. Hatred for the United States exists in the Middle East. It is not new, nor is a driving factor in that hatred blasphemy.[311] The Islamic fundamentalists/extremists will harbor hatred for the United States regardless of what the U.S. position is on free speech. Even if the United States moderates its foreign policy position on freedom of expression, the attacks on the United States and its interests will continue. A change in the U.S. foreign policy would only generate a minor improvement (at best) in some Islamic terrorists' views of the United States, but not enough to eradicate Islamic terrorism, or thereby to justify a change in U.S. policy. Even if the United States were to change its foreign policy, that change will not stop the speech that emanates from the United States. As President Obama said, one person with a smart phone is capable of sending a message of hate, or love, around the world instantly.[312] That message could have positive or negative effects; the internet often brings unpredictable results.[313] The internet is here to stay, and the ability to completely control information is gone with it. Free speech can, and does, do good. There are benefits to mankind, with the Arab Spring only a recent example of the power of speech. The U.S. position on the freedom of expression should stand as a beacon of hope, freedom, and expansive human rights around the world. That beacon should never be diminished.

> world with modern technologies, for us to respond in that way to hateful speech empowers any individual who engages in such speech to create chaos around the world. We empower the worst of us if that's how we respond.

*Id.*

[311] *See* Beeman, *supra* note 294, and Young, *supra* note 296.

[312] *See Obama's Speech to the United Nations General Assembly—Text*, *supra* note 310.

[313] *See, e.g.*, *What's in a Meme? YouTube Causes Upset on 125th Street*, The Economist, Mar. 9, 2013, http://www.economist.com/news/united-states/21573168-youtube-causes-upset-125th-street-whats-meme (discussing the unexpected popularity of the Harlem Shake videos around the world).

# CYBER NEUTRALITY: A TEXTUAL ANALYSIS OF TRADITIONAL JUS IN BELLO NEUTRALITY RULES THROUGH A PURPOSE-BASED LENS

*Major Zachary P. Augustine**



* Maj Zachary P. Augustine, Judge Advocate, United States Air Force (LL.M., Space, Cyber and Telecommunications Law, University of Nebraska-Lincoln (2013); J.D., *summa cum laude*, Northern Illinois University School of Law (2008); B.S., *Distinguished Graduate*, United States Air Force Academy (2002)) is currently deployed to the Combined Air Operations Center, Al Udeid AB, Qatar and permanently assigned as the Chief of Cyber Operations Law, 24th Air Force/Air Force Cyber Command, Joint Base San Antonio-Lackland, Texas. Previous assignments include Acquisitions Officer, Los Angeles Air Force Base, CA; Chief of Military Justice and Chief of Legal Assistance, 28th Bomb Wing, Ellsworth AFB, SD; Chief of Civil Law and Chief of Operations Law, 18th Wing, Kadena AB, Okinawa, Japan. This article was submitted in partial satisfaction of the requirements for the degree of Master of Laws in Space, Cyber, and Telecommunications Law at the University of Nebraska School of Law. The author wishes to thank the faculty and staff at the University of Nebraska for their keen insight into the cyber domain and excellent feedback in drafting this article. The views expressed in this article are solely those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or U.S. Government.

## I. INTRODUCTION

> All warfare is based on deception. Hence, when able to attack, we must seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near—Sun Tzu, *The Art of War*

Whether it was using inflatable tanks to confuse Nazis forces as to the location of the D-Day invasion in World War II[1] or allowing the media to incorrectly conclude and broadcast reports of an imminent amphibious assault on Iraqi forces in Kuwait during the Persian Gulf War,[2] deception has persistently remained a fundamental aspect of warfare. However, the major technological developments of the late 20th and early 21st centuries now allow for deception on a whole new scale. The ability to anonymously mislead an adversary or create harmful effects on an adversary from an ocean away through a few computer keystrokes would probably put a grin on Sun Tzu's face. Today's digitally networked world offers truly amazing benefits on a global scale but also creates newfound vulnerabilities. This has led to what some have referred to as a cyber arms race,[3] where states are increasingly looking to exploit cyber vulnerabilities as a primary instrument of national power. Iran has been heavily investing in cyber capabilities.[4] Russia and China are widely known as major actors in cyberspace.[5] Apparent leaks from highly placed United States government officials suggested that United States and Israeli cyber experts co-developed a malware program, nicknamed Stuxnet, to disrupt operations at Iran's Natanz uranium enrichment facility.[6] With a fairly substantial list of benefits, including the inherent deniability of the Internet, it is easy to see why cyber operations are gaining international popularity, a trend that is likely to continue.[7]

---

[1] U.S. Army Center of Military History, Publ'n No. 72-18, Normandy, p. 15, (*available at* http://www.history.army.mil/html/books/072/72-18/CMH_Pub_72-18.pdf).

[2] John S. Brown, *The Maturation of Operational Art: Operations Desert Shield and Desert Storm*, *in* Historical Perspectives of the Operational Art 439, 460 (U.S. Army Center of Military History, 2005) (*available at* http://www.history.army.mil/html/books/070/70-89-1/cmhPub_70-89.pdf).

[3] *Code Wars*, Wash. Post, June 4, 2012 (*available at* http://articles.washingtonpost.com/2012-06-03/opinions/35462276_1_cyber-security-computer-worm-nuclear-enrichment).

[4] Shaun Waterman, *U.S. Seen as Iran 'Cyberarmy' Target*, Wash. Times, Apr. 25, 2012 (*available at* http://www.washingtontimes.com/news/2012/apr/25/us-seen-as-iran-cyberarmy-target/?page=all).

[5] Ellen Nakashima, *U.S. Said to be Target of Massive Cyber-Espionage Campaign*, Wash. Post, Feb. 11, 2013, (*available at* http://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_print.html).

[6] Ellen Nakashima, Joby Warrick, *Stuxnet was Work of U.S. and Israeli Experts, Officials Say*, Wash. Post, June 1, 2012, (*available at* http://articles.washingtonpost.com/2012-06-01/world/35459494_1_nuclear-program-stuxnet-senior-iranian-officials).

[7] *See, e.g.*, *Pentagon to Boost Cybersecurity Force*, Wash. Post, Jan. 19, 2013, (*available at* http://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-

Along with its benefits, military uses of cyberspace present a number of legal challenges, both internationally and domestically. One key challenge is the difficulty of gaining international consensus on whether traditional laws of armed conflict apply to cyber operations. This article will analyze one of the traditional international rules of armed conflict that might limit a primary benefit of cyber operations: the ability to deceive an adversary. The law of neutrality limits certain deceptive behavior in traditional armed conflict. Maneuvering military forces and weaponry along unexpected routes to surprise an enemy has been a staple of warfare throughout history and is a legitimate form of deception so long as the route does not pass through a neutral state. Does this limitation also prevent maneuvering cyber "forces" or "weaponry" through a neutral state?

Part II of this article will highlight the key neutrality rules that are potentially relevant to activities in cyberspace and then analyze the applicability of these rules to a belligerent's cyber operations. Part III will discuss international standards of attribution and where those standards might present practical problems in applying neutrality rules to cyber activities. Part IV will analyze the potential neutrality implications of several recently reported malicious cyber activities. Part V concludes that neutrality rules do place limits on deceptive cyber practices in an armed conflict. But, while individual belligerents generally have the ability to apply neutrality rules to their own conduct in the cyber domain, neutral states will have difficulty establishing neutrality violations by belligerents and will likely have to rely on notifications from the belligerents themselves.

## II. NEUTRALITY

Modern neutrality rules flow from the Hague Conventions of 1899 and 1907 and derive from a general desire to localize conflict and prevent its spread. States who wish to remain neutral in any given conflict are obligated to take certain precautions so as to avoid improperly assisting a party to the conflict. In exchange for taking these precautions, belligerent states promise to respect the territory and citizens of neutral states. On paper, it is a fairly simple concept. However, in practice, the desire for belligerents to gain tactical, operational, and strategic advantages may test respect for neutrality, especially where violations are difficult to detect.[8]

### A. Neutrality Rules—Hague Conventions of 1899 and 1907

The 1899 and 1907 Hague conferences included a number of conventions related to resolving international disputes and proper behavior during international conflicts. Two of these conventions, Hague V and Hague XIII, were specifically

force/2013/01/19/d87d9dc2-5fec-11e2-b05a-605528f6b712_story_1.html); Waterman, *supra* note 4.

[8] For example, North Vietnamese troops used the dense terrain in Cambodia during the Vietnam War for sanctuary, movement of reinforcements, and communication purposes. Roderick Ogley, The Theory and Practice of Neutrality in the Twentieth Century 199 (1970).

directed at articulating the rights and obligations of neutral states as well as the rights and obligations of belligerents towards neutral states. Hague V dealt with the concepts of neutrality for land warfare while Hague XIII dealt with neutrality rules at sea. These two conventions are still good law today[9] and form the analytical framework for applying neutrality concepts to conflicts in cyberspace.

1. Hague V: Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land

Article 1 of the Hague V articulates the key benefit for neutral states: "the territory of neutral Powers is inviolable."[10] The principle of territorial sovereignty is a hallmark of modern international relations but it can be difficult to apply when cyber capabilities start complementing traditional tools of war. Launching an air attack through a neutral state's sovereign airspace on the way to a target is a clear violation of Article 1[11] but it is much less clear when it comes to routing a malicious cyber activity through a neutral state's infrastructure on the way to the same target.[12]

Article 2 forbids the movement of "troops or convoys of either munitions of war or supplies across the territory of a neutral Power."[13] Here, the term "convoy of munitions" could arguably include cyber weapons but the drafters of this article envisioned the movement of physical weapons over a neutral state's territory.[14]

Article 3 prohibits belligerents from erecting on the "territory of a neutral Power a wireless telegraphy station or apparatus for the purpose of communicating with belligerent forces on land or sea" or using "any installation of this kind established by them before the war on the territory of a neutral Power for purely military purposes, and which has not been opened for the service of public messages."[15] In the cyber context, this raises interesting questions about whether a virtual "wireless telegraphy station" would be prohibited if it could essentially perform the same function as a physical telegraphy station.

---

[9] U.S. Dep't of State, Treaties in Force: A List of Treaties and Other International Agreements of the United States in Force on January 1, 2013, at 479-480 (2013) (*available at* http://www.state.gov/documents/organization/218912.pdf).

[10] Convention Respecting the Rights and Duties of Neutral Powers and Persons In Case of War on Land, art. 1, Oct 18, 1907, 36 Stat. 2310 [hereinafter Hague V].

[11] Int'l & Operational Law Dep't, The Judge Advocate Gen.'s Legal Ctr. & Sch., U.S. Army, JA 422, Operational Law Handbook, Ch. 2, para. XIII.A.1, at 35(2012) [hereinafter Army Operational Law Handbook].

[12] *See* Hague V, *supra* note 10, art. 8 (creating a neutrality exception when using publicly available communication networks).

[13] Hague V, *supra* note 10, art. 2.

[14] *See* James Brown Scott, The Reports to the Hague Conferences of 1899 and 1907, at 539 (1917) [hereinafter Hague Reports].

[15] Hague V, *supra* note 10, art. 3.

Article 4 prevents belligerents from forming a "corps of combatants…on the territory of a neutral Power to assist the belligerents."[16] Would this prevent a belligerent from forming a botnet[17] on the territory of a neutral that could launch a distributed denial of service (DDoS) attack on enemy command and control networks?

Article 5 highlights the key duty of a neutral power, namely to prevent belligerents from performing any of the actions prohibited in Articles 2 through 4.[18] Neutral states may even be required to apply force to comply with these duties.[19] Practically speaking, how could a neutral state prevent belligerents from using its infrastructure if belligerent cyber activities amounted to a violation of Article 2, 3, or 4?

Article 8 lays out an important exception when it comes to the applicability of Hague V to cyber operations. Article 8 says "[a] neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals."[20] While a neutral state does not have to prevent the use of telegraph or telephone lines by belligerents, there is still an obligation to allow equal use by belligerents. Article 9 says "[e]very measure of restriction or prohibition taken by a neutral Power in regard to the matters referred to in Articles 7 and 8 must be impartially applied by it to both belligerents."[21] Additionally, this impartiality requirement flows to private companies who may own or operate communication infrastructure. Article 9 goes on to say "[a] neutral Power must see to the same obligation being observed by companies or private individuals owning telegraph or telephone cables or wireless telegraphy apparatus."[22] One approach would be to cite this exception as blanket authority for a belligerent to use a neutral state's infrastructure to transport malicious cyber code. However, reading this exception too broadly would tend to contravene the purposes of the neutrality rules and other articles arguably support a much more narrow reading of Article 8. Additionally, much of the rationale behind Article 8 seems to stem from the practical problems associated with preventing belligerents from using publicly available communica-

[16] *Id.*, *supra* note 10, art. 4.

[17] "[A] botnet is a large number of compromised computers that are used to generate spam, relay viruses or flood a network or Web server with excessive requests to cause it to fail . . . The computer is compromised via a Trojan that often works by opening an Internet Relay Chat (IRC) channel that waits for commands from the person in control of the botnet. There is a thriving botnet business selling lists of compromised computers to hackers and spammers." PC Magazine Online Dictionary, *available at* http://www.pcmag.com/encyclopedia_term/0,2542,t=botnet&i=38866,00.asp.

[18] Hague V, *supra* note 10, art. 5.

[19] *Id.* at art. 10.

[20] *Id.* at art. 8.

[21] *Id.* at art. 9.

[22] *Id.* at art. 9.

tion lines.[23] The official report of the 1907 Hague conference states that requiring neutrals to prevent belligerents from using these lines would encounter "objections of a practical kind . . . arising out of the considerable difficulties in exercising control, not to mention the confidential character of telegraphic correspondence and the rapidity necessary to this service."[24] If modern technology can diminish some of those enforcement concerns, it would seem to make less sense to interpret Article 8 as sanctioning offensive cyber operations.

2. Hague XIII: Respecting the Rights and Duties of Neutral Powers in Naval War

While Hague XIII offers much less in the way of rules that are relevant to the cyber domain, certain provisions do help guide interpretations of Hague V. The main focus of Hague XIII is to regulate the manner in which belligerent warships may replenish at the ports of neutral states or transit their territorial waters. Mere transit through territorial waters is allowed,[25] while the arming of a vessel at the port of a neutral state is prohibited.[26] Article 5 restates a similar prohibition from Hague V, prohibiting belligerents from using "neutral ports and waters as a base of naval operations against their adversaries" or "erect[ing] wireless telegraphy stations or any apparatus for the purpose of communicating with the belligerent forces on land or sea."[27] Again, it seems to be the *control and operation* of a communication system on the territory (or in the territorial waters) of a neutral state versus the *mere use* of a public utility that is prohibited.

B. When do Neutrality Rules Apply in General?

Before analyzing the applicability of neutrality rules to cyber operations, it is helpful to define the general applicability of neutrality rules in traditional armed conflict. Even if neutrality rules apply to activities in cyberspace, the traditional limitations on neutrality rules will apply as well.

1. International Armed Conflict vs. Non-international Armed Conflict

Strictly speaking, the provisions of Hague V and Hague XIII only apply to international armed conflicts (IAC) between signatory nations.[28] While initially limited to state parties,[29] the provisions of Hague V and Hague XIII are also now

---

[23] *See* Hague Reports, *supra* note 14, at 543.

[24] *Id.*

[25] Convention Concerning the Rights and Duties of Neutral Powers in Naval War art. 10, Oct. 18, 1907, 36 Stat. 2415 [hereinafter Hague XIII].

[26] Hague XIII, *supra* note 25, art 8.

[27] Hague XIII, *supra* note 25, art 5.

[28] *See* Hague V, *supra* note 10, art. 20; Hague XIII, *supra* note 25, art. 28.

[29] *Id.*

binding on all states as customary international law.[30] Formal neutrality rights and obligations only arise when there is a recognized state of belligerency.[31] Belligerency is defined as a state of war between two sovereign states.[32] However, neutrality rights and obligations will also arise in a civil war when foreign states recognize an insurgent force as a belligerent, essentially putting the insurgent force on equal footing with the established government.[33]

A civil war is by definition, a non-international armed conflict (NIAC).[34] However, just because neutrality rights and obligations arise during a civil war does not mean they apply in all types of NIACs. While some authors have argued that neutrality applies in all NIACs,[35] the better view is that recognized civil wars are the only type of NIAC where formal neutrality rules apply.[36] However, the inapplicability of formal neutrality rules to a NIAC does not mean that "neutral" states have no obligations with respect to the conflict participants. Apart from neutrality obligations, states owe each other a general duty to prevent their territory from being used in a way that causes harm to another state. In its first case, the International Court of Justice held that all states have an "obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."[37] This obligation applies at all times and therefore equally to IACs and NIACs. This obligation is only owed to other states, not to insurgencies, essentially creating something analogous to very basic neutrality obligations with respect to the legitimate government but not with respect to the insurgency.[38]

---

[30] Wolff Heintschel von Heinegg, *Neutrality in Cyberspace*, in 4th Conference on Cyber Warfare Proceedings 35, 38 (C. Czosseck, R. Ottis, K. Ziolkowski eds., 2012); Tess Bridgeman, Note, *The Law of Neutrality and the Conflict with Al Qaeda*, 85 Vol 5 N.Y.U. L. Rev. 1186, 1198 (2010).

[31] L. Oppenheim, International Law: A Treatise. Volume II: Disputes, War and Neutrality *§§ 307, 311a, 312 (*7th ed., H. Lauterpact ed., 1952) ("recognition of belligerency alone brings about the operation of rules of neutrality") ("Neutrality ends with the cessation of war").

[32] Black's Law Dictionary 175 (9th ed. 2009) (Belligerency is defined as "[t]he status assumed by a nation that wages war against another nation" and "the act or state of waging war.").

[33] Oppenheim, International Law, *supra* note 31, *§ 308* ("As civil war becomes real war through recognition of the insurgents as a belligerent Power, neutrality during a civil war begins for every foreign State from the moment recognition is granted.").

[34] Michael N. Schmitt, Yoram Dinstein & Charles H.B. Garraway, *The Manual on the Law of Non-International Armed Conflict: With Commentary*, International Institute of Humanitarian Law at 2 (2006), *available at* http://www.iihl.org/iihl/Documents/The%20Manual%20on%20the%20Law%20of%20NIAC.pdf.

[35] Brideman, *supra* note 30, at 1211-1212.

[36] Kevin J. Heller, *The Law of Neutrality Does not Apply to the Conflict with Al-Qaeda, and it's a Good Thing, Too: A Response to Chang*, 47 Tex. Int'l. L.J. 115, 120-21 (2011).

[37] Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 22 (Apr. 9) [hereinafter Corfu Channel Case].

[38] *See* Heller, *supra* note 36, at 119-20; *see e.g.*, Detlev F. Vagts, *The Traditional Concept of Neutrality in a Changing Environment*, 14 Am. U. Intl'l L. Rev. 83, 90-91 (1998); *but see* Karl S. Chang, *Enemy Status and Military Detention in the War Against Al-Qaeda*, 47 Tex Int'l L.J. 1, 40 (2011) (arguing that the neutrality doctrine is applied to insurgencies like al Qaeda).

In the context of cyber operations, the neutrality analysis in part depends on whether the cyber activity itself amounts to an armed conflict or is taking place within the context of a conventional armed conflict. It also depends on the conflict classification as either an IAC or NIAC, made more complicated by the different armed conflict thresholds between the two. The International Committee for the Red Cross Commentary to Article 2 of the Geneva Conventions of 1949 says:

> Any difference arising between two States and leading to the intervention of members of the armed forces is an armed conflict within the meaning of Article 2, even if one of the Parties denies the existence of a state of war. It makes no difference how long the conflict lasts, how much slaughter takes place, or how numerous are the participating forces.[39]

However, for a NIAC, the armed conflict threshold is much higher. Additional Protocol II of the Geneva Conventions of 1949 describes "internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature, as not being armed conflicts."[40]

2. The United Nations Charter and Collective Security Limitations on Neutrality

In addition to properly classifying the nature of a conflict, the practical applicability of neutrality rights and obligations may be limited by commitments under the United Nations (UN) Charter and any other applicable collective security agreements.

(a) *United Nations Charter*

The post-World War II era brought about significant changes to the practical applicability of neutrality rights and obligations, even causing speculation that neutrality would completely disappear.[41] Much of this speculation was based upon the UN Charter's outlawing of war,[42] which is a pre-requisite for neutrality, and on the formal commitment to "give the United Nations every assistance in any action it takes" and "refrain from giving assistance to any state against which the United Nations is taking preventive or enforcement action."[43] With nearly all sovereign

---

[39] Int'l Comm. of the Red Cross, Commentary to the Third Geneva Convention Relative to the Treatment of Prisoners of War 23 (Jean Pictet ed., 1960); *but see* Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 103 (June 27) [hereinafter ICJ Nicaragua Case] (establishing a difference between an armed attack and a "mere frontier incident").

[40] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts, art. 1(2), 8 June 1977, 1125 UNTS 609 [hereinafter Additional Protocol II].

[41] Vagts, *supra* note 38, at 88-89.

[42] U.N. Charter art. 2, para. 3, 4; Vagts, *supra* note 38, at 89.

[43] *Id.* at art. 2, para. 5.

states being members of the United Nations,[44] Article 2(5) would seem to leave little opportunity for states to remain neutral once the United Nations has acted. Under Chapter 7 of the UN Charter, the Security Council has the authority to require[45] all member states to engage in non-forceful actions against an offending state under Article 41 or forceful actions under Article 42.[46] However, the UN Charter's predicted impact in eliminating neutrality has not played out in practice.[47] While the Security Council does have significant enforcement authority, the veto rights[48] held by China, France, Russia, the United Kingdom, and the United States[49] often prevent full use of that authority. Between 1946 and 2012, a permanent member of the UN Security Council used a veto 269 times, though most were cast during the cold war.[50] Because Security Council resolutions require nine of fifteen affirmative votes,[51] including affirmative or abstention votes from all five permanent member states, politics have seemingly prevented the kind of actions that would effectively nullify neutrality opportunities. Instead, Security Council enforcement actions tend to use language like "requests," "invites," "encourages," "authorizes," "endorses," or "urges,"[52] hardly the kind of forceful language that might require a state to abandon a neutrality stance. Even the stronger "calls upon" language sometimes used in Security Council resolutions does not usually equate to a mandate when read in context.[53] Scholars in this area tend to agree that while the Security Council has the potential to drastically limit, or even eliminate, a state's ability to act as a neutral with respect to a particular armed conflict, history suggests that political realities still leave room for neutrality.[54]

---

[44] *See* United Nations membership list *available at* http://www.un.org/en/members/index.shtml.

[45] U.N. Charter art 25 ("The Members of the United Nations agree to accept and carry out the decisions of the Security Council in accordance with the present Charter").

[46] *Id. at* art. 41, 42.

[47] *See generally*, Vagts, *supra* note 38 at 89.

[48] U.N. Charter art. 27, para. 3.

[49] *Id.* at art. 23, para. 1.

[50] *See* Global Policy Forum, Changing Patterns in the Use of the Veto in the Security Council, *available at* http://www.globalpolicy.org/images/pdfs/Changing_Patterns_in_the_Use_of_the_Veto_as_of_August_2012.pdf.

[51] U.N. Charter art. 27, para. 2.

[52] *See*, *e.g.*, S.C. Res 665, U.N. Doc. S/RES/665 (Aug. 25, 1990) (*inviting* member states to participate and *requesting* they provide assistance to Kuwait); S.C. Res 1199, U.N. Doc. S/RES/1199 (Sept. 23, 1998) (*endorsing* international monitoring efforts in Kosovo and *urging* states to make personnel available to continuously monitor the situation); S.C. Res 1378, U.N. Doc. S/RES/1378 (Nov. 14, 2001) (*encouraging* member states to support Afghan security); S.C. Res. 1973, U.N. Doc. S/RES/1973 (Mar. 17, 2011) (*authorizing* member states to take all necessary measures to enforce no-fly zone in Libya).

[53] *See, e.g.*, S.C. Res 665, U.N. Doc. S/RES/665 (Aug. 25, 1990) (calling on "*those states cooperating with the government of Kuwait*" (emphasis added)); S.C. Res 1386, U.N. Doc. S/RES/1386 (Dec. 20, 2001) (calling on member states "*participating in the International Security Assistance Force*" (emphasis added)).

[54] *See, e.g.*, Eric T. Jensen, *Sovereignty and Neutrality in Cyber Conflict*, 35 Fordham Int'l L.J. 815, 820 (2012); Bridgeman, *supra* note 30, at 1208-09; George K. Walker, *Information Warfare*

(b) *Other Collective Security Agreements*

However, even if the UN Security Council fails to take action, or takes action that allows for optional participation, regional security agreements may still prevent a neutral stance. For example, all members[55] of the North Atlantic Treaty Organization (NATO) have agreed that "an armed attack against one or more of them in Europe or North America shall be considered an attack against them all."[56] This language is somewhat softened by Article 5 though, arguably leaving at least some room for states to make individual decisions concerning participation in hostilities. Article 5 says that each member state "will assist the Party or Parties so attacked by *taking…such action as it deems necessary*, including the use of armed force, to restore and maintain the security of the North Atlantic area."[57] By allowing each state to take such action as it deems necessary, there may be some wiggle room for individual NATO states to stay out of a particular conflict without breaching their NATO obligations.

In addition to NATO, there are many other collective security agreements that may limit a state's neutrality options. For example, the United States has committed to the collective defense of nearly thirty countries outside of NATO. The United States, Australia, and New Zealand have a collective security agreement that covers armed attacks in the Pacific Area.[58] The United States has bilateral security agreements with Japan,[59] South Korea,[60] and the Philippines[61] that all address armed attacks in the Pacific against either party. The Southeast Asia Treaty between the United States, United Kingdom, France, Australia, New Zealand, Philippines, and Thailand, says all states will collectively respond to armed attacks in the treaty area as determined by their own "constitutional processes."[62] The Inter-American Treaty of Reciprocal Assistance (Rio Treaty) between 22 North, Central, and South American states says that each signatory nation will "undertake to assist" in meeting

---

*and Neutrality*, 33 Vand. J. Transnat'l L. 1079, 1111 (2000).

[55] Albania, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Turkey, United Kingdom, United States. See current NATO member list *available at* http://www.nato.int/cps/en/natolive/nato_countries.htm.

[56] North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.

[57] *Id.* (emphasis added).

[58] The Australia, New Zealand and United States Security Treaty, Sept. 1, 1951, 3 U.S.T. 3420, 131 U.N.T.S. 83.

[59] Treaty of Mutual Cooperation and Security Between Japan and the United States of America, Jan. 19, 1960, 11 U.S.T. 1632.

[60] Mutual Defense Treaty Between the United States and the Republic of Korea, Oct. 1 1953, 5 U.S.T. 2368, 238 U.N.T.S. 199.

[61] Mutual Defense Treaty Between the United States and the Republic of the Philippines, Aug. 30, 1951, U.S.-Phil., 3 U.S.T. 3947, 177 U.N.T.S. 133.

[62] Southeast Asia Collective Defense Treaty, Sept. 8, 1954, art. 9, 6 U.S.T. 81, 209 U.N.T.S. 28.

an armed attack against another signatory nation.[63] Additionally, while not officially recognizing Taiwan as an independent state, the United States has continually expressed its commitment to defend Taiwan.[64]

While the United States has collective security agreements that span the globe and appears destined for belligerency in just about any future IAC, not all states have such widespread commitments. Additionally, aside from the United Nations, most collective security agreements are based on geographic regions, typically only requiring states to give up a neutrality posture when the conflict creeps into their neighborhood. After all, with traditional methods of warfare would it really matter whether Costa Rica is willing to allow convoys of troops or munitions to cross its territory in support of an armed conflict in Europe? With the interconnected nature of global networks and the development of offensive cyber tools, all of a sudden Costa Rica's stance on a distant European or Asian conflict could become relevant. If neutrality rights and obligations extend to activities in cyberspace, regional security agreements will do very little to eliminate neutrality issues because with global information networks, every state is in the same neighborhood. While the UN Security Council could theoretically require all states to give up a neutrality posture with respect to a particular conflict, practical limitations make it unlikely. So, if all future armed conflicts are going to have at least some neutrals, and all future conflicts will involve cyber operations,[65] how, if at all, do neutrality rules affect activities in cyberspace?

### C. Applying Neutrality Rules in Cyberspace

Even though the Hague V and XIII rules are over a hundred years old, today they provide the basic framework for applying neutrality concepts to activities in cyberspace. There may not be universal international agreement in applying fundamental principles of international law to activities in cyberspace but the United States' position is that existing international law does apply in cyberspace.[66] Additionally, the International Court of Justice has suggested that neutrality rules apply to all weapon systems.[67]

---

[63] Inter-American Treaty of Reciprocal Assistance art. 3, Sept. 2, 1947, 62 Stat. 1681, 21 U.N.T.S. 77.

[64] *See* The Taiwan Relations Act, 22 U.S.C. § 3301 (1979).

[65] *See* Jim Garamone, *Lynn: Cyberwarfare Extends Scope of Conflict*, American Forces Press Service, *available at* http://www.defense.gov/news/newsarticle.aspx?id=61107 (Former Deputy Secretary of Defense William Lynn's suggestion that "[a]ny major future conflict will almost certainly include elements of cyberwarfare.").

[66] Harold Honhgu Koh, Legal Advisor of the Dep't of State, Address to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), *available at* http://www.state.gov/s/l/releases/remarks/197924.htm [hereinafter Koh Comments] ("Some have also said that existing international law is not up to the task, and that we need entirely new treaties to impose a unique set of rules on cyberspace. But the United States has made clear our view that established principles of international law *do* apply in cyberspace.")(emphasis added).

[67] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, para.

While the 1907 neutrality rules are not a perfect fit for most cyber activities, they lead to rational conclusions when applied through a purpose-based lens. The preamble of the Hague V does not define the purpose, merely stating the desire to define "more clearly the rights and duties of neutral Powers in case of war on land."[68] The preamble of Hague XIII is similarly void of a clear purpose statement.[69] Generically, the purpose of neutrality is to preserve state's political and territorial sovereignty. More specifically however, the purpose of neutrality is to preserve a state's ability to choose if and when to enter an armed conflict and to minimize the spread of conflict and its harmful effects.[70] This ultimate purpose is reflected in the policy of United States. The United States Navy handbook for the law of naval operations says "[t]he law of neutrality serves to localize war, to limit the conduct of war on both land and sea, and to lessen the impact of war on international commerce."[71] When applying the neutrality rules to activities in cyberspace they must be viewed through this purpose-based lens of limiting the spread of conflict.

While a full analysis of how the use of force and armed attack thresholds under the United Nations Charter apply in cyberspace is beyond the scope of this article, a purpose-based analysis of the neutrality rules relies on the premise that nations can legitimately exercise self-defense rights in the face of certain malicious cyber activities. First, most scholars agree that activities in cyber space can constitute a use of force or an armed attack.[72] Professor Michael Schmitt, a retired Air Force Lieutenant Colonel, is a leading scholar in this area and has advocated a consequence-based approach. He argues that if a malicious cyber activity has similar destructive consequences of a conventional attack then it is mainly a matter of severity in deciding whether the use of force threshold or armed attack threshold has been crossed.[73] The United States has apparently adopted a similar view. In September 2012, Harold Koh, legal advisor to the State Department, stated "[c]yber activities that proximately result in death, injury, or significant destruction would

88 (July 8) ("The Court finds that as in the case of the principles of humanitarian law applicable in armed conflict, international law leaves no doubt that the principle of neutrality, whatever its content, which is of a fundamental character similar to that of the humanitarian principles and rules, is applicable (subject to the relevant provisions of the United Nations Charter), to all international armed conflict, whatever type of weapons might be used.").

[68] *See* Hague V, *supra* note 10, Preamble.

[69] *See* Hague XIII, *supra* note 25, Preamble.

[70] Georgios C. Petrochilos, *The Relevance of Concepts of War and Armed Conflict to the Law of Neutrality*, 31 Vand. J. Transnat'l L. 575, 580 (1998) ("neutrality logically presupposes independence—that is, the legal capacity to determine a state's own position with regard to questions of peace and war.").

[71] The Commander's Handbook on the Law of Naval Operations, para 7-1, Dep't of the Navy, Naval War Pub. No. 1-14M (2007); *see also*, Wolff Heintschel von Heinegg, *supra* note 30, at 39.

[72] Charles J. Dunlap Jr., Maj. Gen. (Ret.), USAF, *Perspectives for Cyber Strategists on Law for Cyberwar*, 5 Strategic Studies Quarterly, at 81, 85 (Spring 2011).

[73] Michael N. Schmitt, *Cyber Operations and the Jus Ad Bellum Revisited*, 56 Vill. L. Rev. 569, 575-76 (2011).

likely be viewed as a use of force."[74] Koh went on to say "[a] State's national right of self-defense, recognized in Article 51 of the UN Charter, may be triggered by computer network activities that amount to an armed attack or imminent threat thereof."[75] While it is unclear to what extent the international community embraces the ability to assert self-defense rights in response to a malicious cyber activity,[76] with the United States taking an unequivocal position and NATO suggesting a similar stance,[77] others may follow.

It is a state's ability to assert self-defense rights under Article 51 of the UN Charter that is so important to the neutrality analysis. If the whole purpose of neutrality is to prevent the spread of war and belligerents can legitimately assert self-defense rights in response to malicious cyber activity, then when a belligerent routes malicious cyber code through a neutral state's infrastructure on the way to the enemy it threatens the stability that the neutrality rules seek to uphold. Unfettered use of a neutral state's infrastructure for malicious cyber operations raises a significant risk that the neutral state will be dragged into the conflict as the victim state seeks to defend itself. In order to achieve its purpose, the neutrality rules need to apply to all military actions that are likely to trigger defensive measures.

It also makes sense for neutrality rules to apply to this situation when viewed from an incentives perspective. In the absence of governing neutrality rules, a belligerent could find great strategic value in bringing a neutral party into a conflict. One way to get a state to abandon neutrality might be to route destructive cyber code through that neutral country, thereby pressuring an opposing belligerent to take action against the neutral's infrastructure. When portions of the neutral state's infrastructure suddenly shut down or other military operations start affecting day-to-day life in that neutral state, political will to join the conflict could increase. Alternatively, if the defender chooses not to engage the neutral state's infrastructure, the attacker may gain an operational safe haven. For the attacking belligerent, this is a win-win situation that uses a neutral's territory to gain a strategic advantage.

In light of these incentives, the neutrality rules should be interpreted as granting rights and imposing duties in cyberspace if the text allows for such an interpretation. However, one clear limitation in the text concerns territorial borders. Even if the rules can be interpreted to apply to cyber activity, the territorial limitations

---

[74] Koh Comments, *supra* note 66.

[75] *Id.*

[76] *See generally* Lt Col. Patrick W. Franzese, *Sovereignty in Cyberspace*, 64 A.F. L. Rev. 1, 5-6 (2009).

[77] *See* Defending the Networks: The NATO Policy on Cyber Defence, N. Atl. Treaty Org. (2011), *available at* http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf (stating ". . . NATO will defend its territory and populations against all threats, including emerging security challenges such as cyber defence" and "NATO will maintain strategic ambiguity as well as flexibility on how to respond to different types of crises that include a cyber component.").

stressed in Hague V will still serve as distinct boundaries in the analysis. The drafters of Hague V specifically considered and rejected the idea of extending a neutral state's duties to areas where it exercises jurisdiction outside of its sovereign territory.[78] In the cyber context, undersea communication cables or communication satellites would therefore always fall outside the scope of any neutrality analysis. However, within a neutral's territory, the Hague V rules allow for reasonable interpretations concerning their applicability to malicious cyber activities. Articles 2–4 offer the strongest arguments for applying neutrality rules in cyberspace while Article 8 stands as the main counter argument.

The key language in Article 2 is "convoy" of "munitions."[79] The Oxford dictionary defines a convoy as "a group of ships or vehicles travelling together, typically one accompanied by armed troops, warships, or other vehicles for protection."[80] The official report of Hague V arguably elaborates on what is meant by the term "convoy" by distinguishing the prohibition in Article 2 with the permissible activity in Article 7. Article 7 says "[a] neutral State is not called upon to prevent the export or transport, on behalf of one or other of the belligerents, of arms, munitions of war, or, in general, of anything which can be of use to an army or a fleet."[81] The key distinction between Article 2 and Article 7 is the identity of the transporter. If the transporter is a belligerent, then Article 2 acts as a complete bar. If the transporter is anyone else, Article 7 applies.[82] The thrust of the Article 7 rationale is to limit the harmful economic effects of war on a neutral state and its population.[83] In the cyber context, the key then is determining the identity of the transporter. Is it the belligerent typing commands that cause the malicious code to take certain paths through the infrastructure of a neutral state or is it the telecommunications service provider whose physical cables or towers transmit bits of information from node to node? Here, the neutral state's network infrastructure is analogous to its roads. If a belligerent drives a convoy of munitions over the roads of a neutral state there is a clear violation of Article 2, even though the neutral state built the roads, decided which directions they will run, how to manage traffic congestion, and whether or how much to charge in tolls. A physical communication network looks very much the same. The service provider laid the cable or built the towers, created particular routes, established various traffic control mechanisms, and may charge a toll for passing traffic over its network. This interpretation is in line with the economic motive behind Article 7. Any economic gain to a service provider in allowing a belligerent to "hire its transport services" is more closely analogous to paying a road toll than hiring truck drivers or shipping companies to transport crates of munitions. Because the goal of Article 7 is to prevent harmful economic impacts to neutral

[78] Hague Reports, *supra* note 14, at 541.

[79] Hague V, *supra* note 10, art. 2.

[80] Oxford Dictionary *available at* http://oxforddictionaries.com/definition/english/convoy.

[81] Hague V, *supra* note 10, art. 7.

[82] Hague Reports, *supra* note 14, at 539.

[83] *Id.* at 542.

states, it should not encompass cyber transport activity, which at most brings only negligible economic gain.

The prohibition in Article 3 also tends to support the application of neutrality rules to cyber operations, although the focus shifts from munitions to communications. The main thrust of Article 3 is to prohibit belligerents from erecting on a neutral's territory "a wireless telegraphy station or any other apparatus for the purpose of communicating with [the] belligerent forces."[84] The official report from the Hague conferences explains that Article 3 is focused on "installation by belligerent parties of stations or apparatus on the territory of the neutral State."[85] Clearly, this language envisions the establishment of physical infrastructure on a neutral's territory. However, it would be odd for the functional equivalent of a wireless telegraphy station to be excluded. Arguably, one of the main reasons for this provision is that military communication lines are legitimate, and often very important, military targets.[86] If belligerents were allowed to shield command and control targets by virtually placing them within a neutral's territory, an enemy would be forced to either violate that neutral's territory or suffer potentially decisive disadvantages. Modern technology allows for virtual communication stations that could physically reside on any computer connected to the Internet. Virtual communication stations would be equally valid for targeting purposes as a brick and mortar station, although the proportionality analysis may be more difficult if it is a dual use target.[87] If Article 3 only prohibits the establishment of physical communication stations, a belligerent is forced to choose between violating neutrality and suffering tactical and strategic disadvantages. From this perspective, Article 3 should be interpreted as prohibiting the establishment of virtual communication stations within a neutral's territory in the same way it prohibits physical communication stations.

Article 4's prohibition on forming "corps of combatants"[88] in a neutral state should also extend to the cyber domain. The rationale again comes back to the purpose of the neutrality rules and the right of a belligerent to attack legitimate military targets. The official report clarifies that it is the "formation of a corps of combatants to assist a belligerent" that is prohibited. Article 4 appears to focus on the creation of a militia-like force in a neutral territory.[89] The term "combatant" makes it more difficult to apply Article 4 in the cyber context than Articles 2 or 3. Articles 2 and 3 are focused on objects, such as convoys and communication centers, which are easier to translate into the cyber domain. Article 4 is directed a specific group of people who qualify as combatants. There is no functional equivalent of

[84] Hague V, *supra* note 10, art. 3.

[85] Hague Reports, *supra* note 14, at 540.

[86] Army Operational Law Handbook, *supra* note 11, Ch. 2 para. IX.A.2.a.(1), at 22.

[87] *Id.* at Ch. 8 para. II.C.3.b.(5), at 135.

[88] Hague V, *supra* note 10, art. 4.

[89] A neutral state is not obligated to prohibit its nationals from crossing the border and offering assistance to a belligerent. Hague V, *supra* note 10, art. 6.

an individual person in cyberspace. However, in the aggregate, a botnet army may have fair comparisons to a "corps of combatants" in certain situations. Both are organized, have a chain of command, execute the orders of superiors, and can cause appreciable harm to an enemy in carrying out those orders. If both a botnet army and a corps of combatants can accomplish similar military objectives, Article 4 should apply equally to both groups. An enemy belligerent needs to have the same ability to fend off attacks from digital armies as it does human armies, at least to the extent that digital armies can inflict comparable harm. If the goal is to prevent the spread of conflict by localizing war, neither human nor digital armies can have a legal safe haven in neutral states.

While Articles 2–4 allow for reasonable arguments concerning their applicability to cyber operations, Article 8 offers the strongest support for the counter argument. Article 8 does not require neutral states to forbid belligerents to use "telegraph or telephone cables" or any "wireless telegraphy apparatus."[90] Importantly, the text of Article 8 is entirely focused on the neutral state and does not grant any rights to belligerents. In theory, a neutral state certainly could prohibit the use of its communication networks by a belligerent without implicating Article 8. However, the practical difficulties of enforcing such a prohibition would be difficult at best. The Hague report explains that the focus of Article 8 is "the transmission of news," comparing it to a public service.[91] At the time, communication networks had very limited capability. Communicating information was all these early networks could do. Today's network capabilities far exceed the scope of what the drafters of Article 8 likely meant by "the transmission of news" in 1907. While technically speaking, today's networks are still transmitting information in the form of bits and bytes, informing (or misinforming) a human mind on the other end is no longer the sole purpose. The reach of today's automated networks, and automated systems attached to networks, drastically increases the range of achievable effects by merely transmitting information from point A to point B. When the transmission of information has the ability to directly cause physical damage in the real world, Article 8 is no longer merely shielding the flow of information that may be used in planning an attack on the enemy, it is shielding the attack itself.

From a practical standpoint, because Article 8 does not convey any rights to belligerents, a belligerent's ability to invoke Article 51 rights against a neutral state from which malicious cyber operations are emanating may entice neutral states to prohibit belligerents from using their networks at all. However, due to the attribution problems in cyberspace, neutral states may have significant enforcement difficulties in applying an ad hoc approach. Interpreting the rules to place the duty on all belligerents from the outset has the advantages of uniformity and predictability, even if attribution and enforcement problems remain.

---

[90] Hague V, *supra* note 10, art. 8.

[91] Hague Reports, *supra* note 14, at 543.

In order to achieve the purpose of the neutrality rules, belligerents should not be able to exploit the network infrastructure of neutral states. Since the key language of Hague V in Articles 2, 3, 4, 7, and 8, allow for reasonable application to cyber operations, they should be interpreted broadly where doing so is necessary to limit the spread of conflict.

## III. ATTRIBUTION: LEGAL THEORY AND PRACTICE

Meaningful application of neutrality rules requires an enforcement mechanism, especially when gray areas in the law allow for reasonable minds to differ. This part will discuss the international standards of state attribution and briefly analyze some of the practical problems they create for enforcement of neutrality rules in cyberspace. In laying out the standards of state responsibility, this part will first address several legal theories of attribution articulated in the Draft Articles of State Responsibility for Internationally Wrongful Acts and discuss two key International Court of Justice (ICJ) opinions that deal with the factual application of attribution theories. Next, this part will briefly discuss some of the technological features of modern networks that create hurdles in applying these standards to cyber activities.

### A. Legal Theories of State Responsibility

The purpose of the Draft Articles is to codify "the basic rules of international law concerning the responsibility of states for their internationally wrongful acts."[92] Attributing an act to a state has two key components: a valid legal theory of attribution and identification of the actor. Articles 4 through 11 of the Draft Articles contain different legal theories of attribution, all of which could be applied in the cyber context. However, this section will focus on Articles 4, 5, 7, and 8.

Article 4 of the Draft Articles is the most direct legal theory of attribution. It holds a state responsible for the actions of "any State organ," which includes "any person or entity."[93]

Article 5 extends responsibility to the state when the state has empowered a non-state organ by law to "exercise elements of governmental authority."[94] Entities empowered by a state would include publicly or state owned companies.[95] If those public companies are empowered by law to exercise elements of governmental authority, then their actions are attributable to the state. Border control is a typical state function. If a government owned information service provider has

---

[92] U.N. Int'l Law Comm'n, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, p. 31, in Rep. of the Int'l Law Comm'n, 53rd Sess., April 23-June 1, July 2-Aug. 10, 2001, U.N. Doc. A/56/10; U.N. GAOR, 56th Sess., Supp. No. 10 (2001) [hereinafter Draft Articles on State Responsibility].

[93] *Id.* at art. 4.

[94] *Id.* at art. 5.

[95] *Id.* at art. 5 commentary, para. 2.

been empowered by law to conduct digital border inspections, any internationally wrongful actions it takes while performing that border control function are arguably attributable to the state.

These actions are attributable to the state even if the entity exceeds its authority or directly contravenes state law, as articulated in Article 7.[96] Article 7's extension of state responsibility to unauthorized acts applies to both a state organ and to an entity empowered by state law. It prevents a state from taking "refuge behind the notion that, according to the provisions of its internal law or to instructions which may have been given to its organs or agents, their actions or omissions ought not to have occurred or ought to have taken a different form."[97]

Article 8 of the Draft Articles states an important theory of attribution for cyber operations but presents difficult practical problems. Article 8 says the "conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."[98] A key distinction between Article 8 and Article 5 is that Article 8 requires a state law that confers authority while Article 5 applies to less formal ties between the state and the actor.[99] Article 8 applies where "individuals or groups of private individuals who, though not specifically commissioned by the State and not forming part of its police or armed forces, are employed as auxiliaries or are sent as 'volunteers' to neighboring countries, or who are instructed to carry out particular missions abroad."[100] Article 8 encompasses the direction or control standard reflected in the ICJ's holding in the *Military and Paramilitary Activities in and against Nicaragua* case. In that case, Nicaragua attempted to hold the United States responsible for various humanitarian violations committed by an organized anti-government group.[101] While the ICJ found that the United States had trained, equipped, supplied, and financed these anti-government groups, there was no evidence that the United States *directed* or *controlled* the particular humanitarian violations alleged.[102] The court stated that for the United States to be held liable for the particular humanitarian violations "it would in principle have to be proved that that State had effective control of the military or paramilitary operations in the course of which the alleged violations were committed."[103] However, the court did hold that "the United States of America, by training, arming, equipping, financing and supplying the contra forces or otherwise encouraging, supporting and aiding military and paramilitary activities…has acted…

---

[96] *Id.* at art. 7.

[97] *Id.* at art. 7 commentary, para. 2.

[98] *Id. at* art. 8.

[99] *Id.* at art. 5 commentary, para. 7.

[100] *Id.* at art. 8 commentary, para. 2.

[101] *See* ICJ Nicaragua Case, *supra* 39, at 6.

[102] *Id.* at 315.

[103] *Id.* at 115.

in breach of its obligation under customary international law not to intervene in the affairs of another State."[104]

The commentary to Article 8 suggests that a state will be liable when it either actually participates in the operation or gives specific directions concerning the operation.[105] In applying this standard to operations in cyberspace, the general funding, training, or supplying of non-state entities who are engaged in malicious cyber activity might constitute a violation of the non-intervention principle but would not amount to directing or controlling specific operations. Directing specific types of malicious cyber activities against specific targets, would likely meet the direction or control threshold with respect to the end result, but it might not meet the direction or control threshold for the manner of delivery. This could lead to a situation where a state directed or controlled a specific act because of its involvement in the specific malicious software and the choosing of targets, but did not direct or control its delivery through a neutral state.

Another theory of attribution with particular relevance to cyber operations is based on the ICJ's rationale in the Corfu Channel case. This theory would be included under Article 4 of the Draft Articles as "conduct" of a state organ. In the Corfu Channel case, the ICJ held Albania liable for failing to warn British ships of the presence of mines in its territorial waters.[106] The court reasoned that Albania's knowledge of the presence of the mines, regardless of who put them there, established liability.[107] Importantly, there was no direct evidence of Albania's knowledge. The court was willing to infer knowledge, provided the inferences left "no room for reasonable doubt."[108] The court was careful to state that "it cannot be concluded from the mere fact of the control exercised by a State over its territory and waters that that State necessarily knew, or ought to have known, of any unlawful act perpetrated therein."[109] The court relied on strong evidence that Albania continuously kept a close watch over its territorial waters in the Corfu Channel and the laying of mines in those waters would have likely been discovered by Albanian authorities.[110] This theory is particularly enticing in the cyber context, especially when a government exercises tight control over its information networks, and is frequently cited by authors as a potential partial solution to the attribution problem.[111]

---

[104] ICJ Nicaragua Case, at 146.

[105] Draft Articles on State Responsibility, *supra* note 92, art. 8 commentary, para. 3-4.

[106] Corfu Channel Case, *supra* note 37.

[107] *Id.* at 18.

[108] *Id.* at 18.

[109] *Id.* at 18.

[110] *Id.* at 18-20.

[111] *See, e.g.*, Scott J. Shackleford and Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 Geo J. Int'l L. 971, 989 (2011); Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel, *The Law of Cyber Attack*, 100 Cal. L. Rev. 817, 855 (2012).

B. Technical and Human Attribution

Attribution is most appropriately divided into two subcategories: technical attribution and human attribution. Technical attribution is tracing the physical path of the code to the computer at its source. Human attribution is identifying the person operating the computer. In reality, only the human attribution aspect is necessary to apply a legal theory of attribution but because of the ability to mask identity on the Internet, it may be impossible to conclusively establish human attribution without combining the technical component. Additionally, strong evidence of technical attribution may allow for an inference of knowledge based on Corfu Channel's rationale, especially where a state organ exercises significant control over Internet traffic and infrastructure.

Technical attribution is a significant challenge in applying any legal standard to cyber operations. The Internet's design encompasses a fundamental tradeoff, choosing the free flow of information over security. At times, U.S. government officials have called for the design of a new version of the Internet for critical infrastructure that primarily focuses on security.[112] A more secure Internet would likely make technical attribution easier but until one is developed, sophisticated cyber operators will continue to exploit the anonymity offered by the current version.

The ability to technically attribute an action in cyberspace may significantly depend on the type of activity. When information flows across the Internet it is broken down into several smaller packets.[113] Each packet contains a destination Internet Protocol (IP) address, a source IP address, and a portion of the message.[114] Each packet is sent from the source computer to an initial router. The initial router reads the destination address and forwards the packet to another router until the packet eventually reaches the destination address.[115]

One of the concerns with technical attribution relates to the source address, which may be faked or "spoofed."[116] While this is legitimate issue, it does not apply to all malicious cyber activities. If the sender wants to receive any information back from the destination address, then the source address contained in the packet must lead back to the sender, even if not directly.[117] While many malicious cyber activities will seek a response, a DDoS attack can be carried out without seeking

---

[112] *See* J. Nicholas Hoover, *Cyber Command Director: U.S. Needs to Secure Critical Infrastructure*, InformationWeek.com, *available at* http://www.informationweek.com/government/security/cyber-command-director-us-needs-to-secur/227500515.

[113] David D. Clark and Susan Landau, Essay, *Untangling Attribution*, 2 Harv. Nat'l Sec. J. 531, 534 (2011).

[114] *Id.*

[115] *Id.*

[116] *Id.* at 534-35.

[117] *Id.*

a response.[118] When the sender's IP address is spoofed, tracing the source may not even be possible.[119]

When the source IP address is not spoofed, technical attribution remains a challenge, even if it may be technically possible. A common technique to frustrate attribution is the use of proxies.[120] Proxies are intermediaries that perform various technical functions for a customer before a message is sent to a destination.[121] Proxies frustrate attribution because they replace the source IP address of all packets with their own IP address.[122] Some proxies are designed solely for the purpose of preserving anonymity[123] and depending on the geographic location of the proxy server, gaining cooperation from its owner/operator, at least through judicial means, may not be possible.

Onion routing is another technique that complicates attribution even when the source IP address is not spoofed. Onion routing is basically a process where a message goes through several intermediaries before it reaches its recipient.[124] However, what makes onion routing unique is that each layer of the transmission is fully encrypted, including the source address, destination address, and contents of the message.[125] Each router is only able to decrypt the address of the next router and is therefore unaware of the source, contents, or ultimate destination.[126] Tor is a publicly available onion routing service[127] and is commonly used by militaries, intelligence agencies, and law enforcement personnel, among others.[128] Further complicating matters, various "anonymizing" techniques can be combined and each technique can have multiple steps.[129]

Despite the availability of these sophisticated techniques, security firms continue to claim success in tracing the origins of various malicious cyber activities. In February 2013, Mandiant, a U.S. computer security firm, released a report tracing systematic hacking efforts dating back to 2006 to hundreds of IP addresses

---

[118] *Id.* at 537-38.

[119] *Id.* at 537.

[120] W. Earl Boebert, *A* Survey *of* Challenges *in* Attribution, *in* Comm. on Deterring Cyberattacks, Nat'l Research Council, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, at 45 (2010), *available at* http://www.nap.edu/catalog/12997.html.

[121] *Id.*

[122] *Id*.

[123] *Id*.

[124] *Id.* at 46.

[125] *Id*.

[126] *Id*.

[127] *Id*.

[128] Clark, *supra* note 113, at 546.

[129] *Id.* at 542-43.

registered in China.[130] According to the report, Chinese hackers frequently hijacked third party computers, using tools such as Remote Desktop, before hacking the target computers.[131] However, Mandiant claims to have traced the link between the hacker and the hijacked computer in 1,905 instances from January 2011 to January 2013.[132] The connection was traced to 832 IP addresses, 817 of which were registered in China and mainly belonged to one of four large blocks of IP addresses that service Shanghai.[133] Chinese authorities have boisterously denied responsibility, calling Mandiant's report "irresponsible and unprofessional."[134] Technical aspects alone should probably not conclusively establish an origination point. As discussed earlier, various techniques allow hackers to mask their true location. Could it be, as Chinese authorities seem to suggest,[135] that hackers outside of China are masking their attacks as originating from China? The Mandiant report did not solely rely on technical analysis. In fact, it combined significant human attribution techniques and other non-technical data to paint a comprehensive picture. For example, two of the four large blocks of IP addresses identified by Mandiant serviced the same area where Chinese Military Unit 61398 is headquartered.[136] According to the report, independent information suggested that Unit 61398 is tasked with computer network operations that specifically target English speaking countries.[137] The remote desktop intrusions were driven by a Chinese virtual keyboard layout setting in 97% of the identified intrusions.[138] The report even identifies several hackers by name through various techniques, such as when hackers logged into their personnel Facebook accounts through the same command and control infrastructure they used to infiltrate intermediary systems.[139] In this case, it is the sheer volume of evidence, both technical and human, that seem to reliably attribute the source.

However, even without the human attribution evidence, an attribution argument based on Corfu Channel's rationale in this case is persuasive. The Chinese government exercises significant control over its communication networks, including cell phones, e-mail, and Internet access.[140] Additionally, because the telecommunica-

---

[130] *See* Mandiant, *APT1 Exposing One of China's Cyber Espionage Units*, at pg.2-6, *available at* http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf [hereinafter Mandiant Report].

[131] *Id.* at 39-40.

[132] *Id.* at 40.

[133] *Id.*

[134] David E. Sanger, David Barboza and Nicole Perlroth, *Chinese Army Unit Seen as Tied to Hacking Against U.S.*, N.Y. Times, Feb. 19, 2013, at A1, *available at* http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html.

[135] *Id*.

[136] Mandiant Report, *supra* note 130, p. 40.

[137] *Id.* at 9.

[138] Mandiant Report, *supra* note 130, p. 4.

[139] *Id.* at 51-58.

[140] Sharon LaFraniere & David Barboza, *China Tightens Censorship of Electronic Communications*, N.Y. Times, Mar. 22, 2011, at A4, *available at* http://www.nytimes.com/2011/03/22/world/asia/22china.html?pagewanted=all&_r=1&.

tions industry in China is state-owned,[141] it would be difficult to argue it did not at least have knowledge of the intrusions.[142] Under Corfu Channel, knowledge coupled with the failure to warn or take other adequate measures to prevent harm, is in itself an internationally wrongful act, regardless of who actually controls the computer.[143]

### C. Attributing Conduct for Neutrality Purposes

Even if attribution is possible for sustained and systematic hacking by a Chinese military unit, it may be very difficult to attribute isolated incidents that could implicate neutrality concerns. However, the utility of an isolated incident might be questionable. The effective deployment of malicious software that could have militarily significant results would likely require extensive intelligence gathering. The intelligence gathering phase of a cyber operation typically requires the same or similar access as the deployment stage. Additionally, because of routine software updates or patches, without continuous monitoring of the target system, the operation has a high risk of failure.

Another practical attribution issue is that a neutral country may not have the same incentive to duplicate Mandiant's rigorous investigative efforts. While belligerents will be highly motivated to discover the source of malicious cyber activity, many neutral states may determine that effective monitoring costs significantly outweigh the benefits, at least until belligerents threaten to expand the battlefield into its territory.

## IV. CASE STUDIES

While there has not yet been an armed conflict between the countries with the most advanced cyber forces, cyber capabilities continue to develop and are increasingly incorporated by military planners. This part will analyze the neutrality implications of different types of cyber operations by looking at several recently reported uses of malicious cyber capabilities. While some of these examples did actually raise neutrality issues, this part will hypothetically build on these examples in order to better explore various legal boundaries.

---

[141] Keith Bradsher, *China's Grip on* Economy *Will* Test New Leaders, N.Y. Times, Nov. 9, 2012, *available at* http://www.nytimes.com/2012/11/10/world/asia/state-enterprises-pose-test-for-chinas-new-leaders.html?pagewanted=all&_r=0.

[142] Cadie Thompson, *Chinese Hacking Defense 'Hard to Believe': Security Expert*, CNBC, *available at http*://www.cnbc.com/id/100470478.

[143] Corfu Channel Case, *supra* note 37, at 18.

## A. Estonia

### 1. Background

The 2007 network intrusions in Estonia demonstrated how disruptive a coordinated cyber campaign can be on a society that is heavily dependent on modern technology. By 2007, Estonia had become one of the most technologically dependent countries in the world. Electronic banking accounted for 95% of all banking operations, 98% of its territory had Internet access, and many government services and functions were primarily conducted online.[144] In April of 2007, political tensions rose between Estonia and Russia after Estonian officials decided to remove a Soviet-era WWII memorial.[145] The decision resulted in local riots in Tallinn, Estonia's capital, mainly among ethnic Russians.[146] Between April 27th and May 18th, Estonia was the victim of numerous malicious and disruptive cyber activities, mainly consisting of website defacement and denial of service (DoS) attacks.[147] These disruptive cyber activities had significant economic and societal effects.[148] While some of the intrusions were traced to IP addresses registered in Moscow, including government institutions, the Russian government denied any involvement and many of the intrusions involved computers from 178 different countries.[149]

### 2. Neutrality Analysis

Because these intrusions into Estonia's networks did not occur during the course of an armed conflict, and did not trigger an armed conflict, they did not raise any formal neutrality issues. However, at least one author has argued that these intrusions collectively could have amounted to an illegal use of force.[150] While Estonia did not invoke NATO's collective defense measures, it is not difficult to imagine a similar cyber operation escalating into an armed conflict or taking place as part of an ongoing conventional armed conflict where formal neutrality rights and obligations would apply.

If the cyber activity in Estonia had escalated to an armed conflict it would have raised significant neutrality issues. Of the 178 countries whose infrastructure was reportedly involved in the intrusions,[151] it is likely that at least some of them would want to take a neutral stance.

---

[144] Eneken Tikk, Kadri Kaska, Liis Vihul, *International Cyber Incidents: Legal Considerations* 17-18 (2010).

[145] Tikk, Kaska, Vihul, *supra* note 144, at 15.

[146] *Id.* at 15.

[147] *Id.* at 18-21.

[148] *Id.* at 24-25.

[149] *Id.* at 23.

[150] Schmitt, *supra* note 73, at 577.

[151] Tikk, Kaska, Vihul, *supra* note 144, at 23.

Most of the malicious cyber activity against Estonia was aimed at denying access, either in the form of DoS attacks or various attacks on Domain Name Servers (DNS). [152] This type of malicious cyber activity is not likely to cause permanent damage to a network or systems on a network and mainly has the effect of hindering information flow. In the context of an armed conflict, belligerents might use this type of capability to help protect conventional forces during an attack by limiting an enemy's ability to effectively communicate. DoS attacks could therefore arguably provide capabilities comparable to electronic jamming systems.

For example, the United States Navy uses the EA-6B as an airborne jamming system to suppress enemy air defenses.[153] The EA-6B is mainly used as a support element of tactical strike packages by disrupting the enemy's electronic signals and allowing strike aircraft or ground troops to hit designated targets with minimal resistance.[154] Another example is the U.S. Army's use of cell phone jammers in Afghanistan. The Army uses mobile jamming systems that emit powerful radio signals that drown out all other signals over a particular area. [155] While preventing remote Improvised Explosive Device (IED) detonations is one of the primary uses of these cell phone jamming systems,[156] they can also be used to support offensive operations by blacking out cell signals in a particular area during an attack.

There is no doubt that positioning an EA-6B or a mobile cell phone jamming system in a neutral country would violate that neutral country's rights.[157] What about a comparable cyber capability? The difference with the cyber capability is that a DoS attack simultaneously comes from so many different places, as illustrated in the Estonia situation. The three options would be to say that neutrality rules do not govern this type of activity at all, they govern every aspect of the activity, or they govern certain parts of the activity.

Because the purpose of neutrality rules is to prevent the spread of conflict,[158] exempting all DoS attacks from neutrality rules is an unsatisfying option. It would put belligerents in the delicate position of choosing between granting safe havens or taking defensive measures that could convince neutral countries to ally themselves with opposing forces. However, because of the way DoS attacks work, often enslaving computers all over the world, fully applying neutrality rules to the activity of

---

[152] Tikk, Kaska, Vihul, *supra* note 144, at 21.

[153] *EA-6B Prowler Mission, Description, and Specifications*, Naval Air Systems Command Website, *available at* http://www.navair.navy.mil/index.cfm?fuseaction=home.display&key=C8B54023-C006-4699-BD20-9A45FBA02B9A (last visited Apr 13, 2013) [hereinafter, EA-6B Details].

[154] *Id.*

[155] David Axe, *Secret Army Bomb Jammers Stolen in Afghanistan*, WIRED, Mar. 1, 2012, *available at* http://www.wired.com/dangerroom/2012/03/bomb-jammers-stolen/.

[156] *Id.*

[157] Hague V, *supra* note 10, art. 2.

[158] *See supra* notes 70-71 and accompanying text.

every computer participating in a DoS attack would be nearly impossible to enforce. Additionally, not all computers participating in a DoS attack carry the same risk of spreading a conflict. A belligerent suffering a debilitating DoS attack in conjunction with a physical attack is much more likely to attack the computers that are controlling a botnet, the command and control node, than the enslaved computers that are merely following orders. Identifying the command and control node may be technically difficult but belligerents are unlikely to expend limited defensive resources unless they are likely to have the desired military effect. For example, using a military option to disable one of the 10,000 enslaved computers will not do much to stop a DoS attack, but focusing a military option against a command and control node could stop the attack altogether.

By applying the neutrality rules only to the activity of the command and control nodes instead of all computers participating in the DoS attack, the purpose of the neutrality rules can be harmonized with some of the practical realities of cyber capabilities. Under this approach, belligerents would be prohibited from using command and control nodes that are geographically located in a neutral country, but not necessarily prohibited from enlisting individual computers in a neutral country to participate in a DoS attack. If a military option could realistically disable all computers participating in the DoS attack, consistent with other LOAC principles, then the neutrality rules should apply to the use of those individual computers as well. As soon as persons or objects within a neutral state become legitimate military targets, the neutrality rules become a vital tool to help limit the spread of conflict.

In Estonia, the DoS attacks apparently began more or less as an unorganized cyber protest but evolved into an organized and sophisticated attack that suggested "central command and control."[159] If this DoS attack had occurred during an armed conflict, it is the location of the command and control nodes that would be most important in conducting the neutrality analysis but there may be situations where the location of the individual computers is important as well. For example, if many of the individual computers participating in a DoS attack were co-located, military options specifically targeting those individual computers might become more realistic.

## B. Georgia

### 1. Background

While the Estonia situation raised many interesting hypothetical situations concerning the applicability of neutrality rules to activities in cyberspace, the Georgia situation in 2008 actually raised neutrality issues. The key distinction in Georgia was that the cyber activity occurred in conjunction with a conventional armed conflict between Russia and Georgia.[160] On August 8, 2008, Russian military

[159] Tikk, Kaska, Vihul, *supra* note 144, at 23.

[160] *Id.* at 67.

forces entered Georgian territory, claiming a need to protect Russian citizens abroad from hostile action by the Georgian military.[161] In response to Russian aggression, Georgia mobilized military forces and declared a state of war.[162] Various malicious cyber activities against Georgian governmental websites also began on August 8,[163] although the Russian government denied all involvement in the cyber activities.[164] While Georgian society was much less dependent on the Internet than Estonian society, various governmental organizations heavily relied on websites to disseminate information.[165] The malicious cyber activity closely paralleled the activity against Estonia a year earlier, mainly consisting of DoS attacks and defacement of public websites.[166] The sites specifically targeted included the Georgian President's website, the central government's website, the Ministry of Foreign Affairs' website, and the Ministry of Defense's website.[167] As in Estonia, the malicious cyber activity originated from all over the world, and was likely carried out by one or more botnets.[168] However, at least one command and control server was traced to an IP address in Turkey.[169]

Another important aspect of the Georgia situation concerns the assistance Georgia received from third parties. Tulip Systems, a private web hosting company based in Atlanta, Georgia, apparently reached out to Georgian government officials after the DoS attacks started and offered to host various government websites.[170] Tulip Systems took these actions without any apparent authorization from the United States Government.[171] The company offered assistance in order to "'protect' the nation of Georgia's Internet sites from malicious traffic."[172] After hosting several key Georgian websites, Tulips Systems was subsequently the target of several DoS attacks.[173]

---

[161] *Id.* at 67.

[162] *Id.* at 68.

[163] *Id.*

[164] *Id.* at 75.

[165] *Id.* at 70.

[166] *Id.* at 71.

[167] Tikk, Kaska, Vihul, *supra* note 144, at 70.

[168] *Id.* at 71.

[169] *Id.* at 70.

[170] Stephen W. Korns, Joshua E. Kasteberg, *Georgia's Cyber Left Hook*, Parameters 61, 66-67 (2009).

[171] *Id.* at 67.

[172] *Id.*

[173] *Id.*

2. Neutrality Analysis

This conflict between Russia and Georgia raised two significant cyber neutrality issues. The first concerns the neutrality rights of Turkey while the second concerns the neutrality rights of the United States.

(a) *Turkish Neutrality*

While Turkey did not formally declare itself to be a neutral in the Russian-Georgian armed conflict, which technically only lasted five days,[174] official Turkish statements suggested a desire to remain neutral. Shortly after the conflict ended, the Turkish Prime minister stated:

> It would not be right for Turkey to be pushed toward any side. Certain circles want to push Turkey into a corner either with the United States or Russia after the Georgian incident. One of the sides is our closest ally, the United States. The other side is Russia, with which we have an important trade volume. We would act in the line with what Turkey's national interests require.[175]

These statements by the Turkish Prime Minister suggest that Turkey did not want to take sides and may have officially declared neutrality had the conflict lasted longer. However, with at least one botnet's command and control server apparently residing in Turkey,[176] Turkish sovereign territory may have played a significant role in the cyber portion of the conflict. Assuming Georgia, or any of its allies, could identify the command and control server in Turkey during the DoS attack, what were Georgia's options? What if the DoS attack was hindering Georgian forces ability to communicate and mount an effective defense against invading Russian forces? Georgian forces would have been in a difficult position, potentially having to choose between taking military action against servers residing in a neutral state or simply accepting the degraded communications environment. This is precisely the type of conundrum the neutrality rules seek to avoid. By treating the command and control server as a neutrality violation, Turkey has an obligation to take necessary action to shut it down if it wants to remain neutral.[177] From Turkey's point of view, treating this as a neutrality violation probably also helps with the complicated political balancing act. Turkey can shut down the command and control server in the name of neutrality and avoid the perception that it is taking sides in the conflict. If the neutrality rules do not apply, any decision Turkey makes may be perceived as taking a side in the conflict. If it shuts down the server, Russia may perceive Turkey

[174] Tikk, Kaska, Vihul, *supra* note 144, at 68.

[175] Igor Torbakov, *The Georgia Crisis and Russia-Turkey Relations*, The Jamestown Foundation, at 20 (2008), *available at* http://www.jamestown.org/uploads/media/GeorgiaCrisisTorbakov.pdf.

[176] Tikk, Kaska, Vihul, *supra* note 144, at 70.

[177] Hague V, *supra* note 10, art. 5.

as taking Georgia's side, while if it leaves the server up and running, Georgia may perceive Turkey as taking Russia's side.

What about attribution? How can Georgia, Turkey or any other interested party know whether Russian forces are operating the command and control server? The reality may be that they cannot know with much certainty, at least not in real time. But does it really matter? Georgia's right to take defensive action against the server does not depend on positively identifying the operator, although the manner in which it exercises that right probably does. While it is true that civilians and civilian objects are protected by the law of armed conflict, civilians may be targeted when they directly participate in hostilities[178] and civilian objects become military objects when used to effectively contribute to military action.[179] From Georgia's perspective, DoS attacks that begin just as Russia invades and inhibit vital communications are arguably making an effective contribution to military action. Georgia may not be able to target specific *personnel* without additional attribution facts, but it likely could target the *object* performing a command and control function for a debilitating DoS attack. Any Georgian response would only be subject to a proper proportionality analysis. Depending on how Georgia conducts its proportionality analysis, it might choose to disable the command and control server with cyber tools or conventional weapons, but either option could theoretically be justified under the law of armed conflict. When the law of armed conflict would allow for a belligerent to take military action against persons or objects in a neutral country, the neutrality rules have to apply if the concept of neutrality is to survive modern warfare.

Furthermore, Hague V textually supports interpreting these command and control servers as constituting neutrality violations. Both Article 2[180] and Article 3[181] could arguably apply to command and control servers but Article 3 is a better fit. A command and control server is closely analogous to a "wireless telegraphy station." The command and control server is used to send and receive messages in much the same way as a telegraphy station would send and receive messages. Additionally, command and control servers clearly communicate with belligerent "forces." Article 2 is specifically directed at convoys of troops or munitions but Article 3 uses the broader term "forces." Even if reasonable minds could differ on whether the individual computers performing the DoS attack are "forces" within the

---

[178] *See* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art 51, June 8, 1977, 1125 UNTS 3 [hereinafter Additional Protocol I].

[179] Id. at art. 52.

[180] Hague V, *supra* note 10, art. 2 ("Belligerents are forbidden to move troops or convoys of either munitions of war or supplies across the territory of a neutral Power.").

[181] Hague V, *supra* note 10, art. 3 (stating that "[b]elligerents are likewise forbidden: (a) To erect on the territory of a neutral Power a wireless telegraphy station or apparatus for the purpose of communicating with belligerent forces on land or sea; (b) To use any installation of this kind established by them before the war on the territory of a neutral Power for purely military purposes, and which has not been opened for the service of public messages.").

meaning of Hague V, the command and control server is also communicating with the person or persons ultimately controlling the botnet. The command and control server has to receive instructions on targets, timing, and duration of the attack that it then sends out to all of the individual computers that make up the botnet. The person or persons ultimately controlling the botnet would likely qualify as a belligerent force, even if only as an unprivileged belligerent force not formally associated with a military.[182] The communication between this belligerent force and the command and control server would then bring the activity within the purview of Article 3.

(b) *United States' Neutrality*

The second main cyber neutrality issue raised by the Russian-Georgian conflict concerns the ability for well-intentioned third parties to threaten their own government's neutrality. When Tulip Systems hosted key Georgian websites in the United States it likely jeopardized the United States' ability to remain neutral.[183] By hosting key governmental websites used for disseminating information, Tulip Systems may have allowed a belligerent to erect "a wireless telegraphy station or apparatus for the purpose of communicating with belligerent forces"[184] on the territory of a potentially neutral state. By not taking action to prevent the hosting of the websites, the United States government may have forfeited its right to remain neutral.[185]

Some might argue that with Russia denying responsibility for the DoS attacks combined with the inherent attribution problems of such attacks, the United States' assistance to Georgia in this situation does not put the United States' neutrality at risk.[186] While this kind of argument might be enticing from a defensive perspective for a country wishing to maintain neutrality, it could significantly undermine a country's offensive options with respect to unlawful combatants or unprivileged combatants in the cyber domain in other conflicts. The law of armed conflict recognizes the ability to lawfully target anyone who takes part in hostilities.[187] In the official commentary to Additional Protocol I, the ICRC defines hostilities as "acts which by their nature and purpose are intended to cause actual harm to the personnel and equipment of the armed forces."[188] It goes on to say that civilians who take "part

[182] For example, the U.S. law defines an unprivileged enemy belligerent as anyone who "has engaged in hostilities against the United States or its coalition partners" or "has purposefully and materially supported hostilities against the United States or its coalition partners." *See* 10 U.S.C. § 948a(7) (2009). Anyone controlling a botnet that appears to act in conjunction with invading conventional forces would almost certainly qualify as one who "has purposely and materially supported hostilities."

[183] Korns, Kasteberg, *supra* note 170, at 68.

[184] Hague V, *supra* note 10, art. 3.

[185] *Id.* at art. 5.

[186] *See* Rain Ottis, *Georgia 2008 and Cyber Neutrality*, *available at* http://conflictsincyberspace.blogspot.com/2010/03/georgia-2008-and-cyber-neutrality.html.

[187] *See* Additional Protocol I, *supra* note 178, art. 51.

[188] Claude Pilloud *et al.,* Claude Pilloud Et Al., Commentary on the Additional Protocols of 8

in armed combat, either individually or as a part of a group" become "a legitimate target."[189] Even if the botnet itself is not intended to cause actual harm it is arguably facilitating the harm that will be caused by the invading conventional forces and therefore could amount to direct participation in hostilities.[190] It would be problematic for a state to argue on the one hand there is no way to know who is behind these DoS attacks and therefore it can render assistance without sacrificing neutrality, and then on the other hand argue this behavior constitutes direct participation in hostilities for targeting purposes in a later conflict. The better view is that when malicious cyber activity augments or enables conventional attacks in an IAC, the cyber component should be treated as belligerent activity. It may be important to sort out whether the malicious cyber activity is privileged belligerent activity or unprivileged belligerent activity in many situations, but it does not matter in the neutrality analysis.

### C. Stuxnet

The previous examples mainly centered on some of the neutrality implications of DoS attacks but the military application of cyber capabilities extends beyond merely preventing access to information. The Stuxnet worm is an example of a cyber capability that can have effects that are comparable to a damage-inflicting conventional weapon, versus effects that are comparable to a damage-enabling conventional capability. Cyber capabilities that could conceivably substitute for conventional damage-inflicting weapons increase the need for applicable neutrality rules.

#### 1. Background

On June 17, 2010, an employee at VirusBlokAda, a small computer security firm in Belarus, read a report from a client in Iran showing that the client's computer was continuously rebooting.[191] The rebooting problem indicated a potential virus and employees at VirusBlokAda soon began analyzing the system for malicious software.[192] They discovered a zero-day exploit in Microsoft's web browser, Internet Explorer.[193] Zero-day exploits are software vulnerabilities that are unknown to its designers and they are quite rare.[194] Software analysis later discovered that Stuxnet took advantage of several additional Windows vulnerabilities, including additional

---

June 1977 to the Geneva Conventions of 12 August 1949, 618 (Yves Sandoz et al. eds., 1987).

[189] *Id.*

[190] *See* Michael N. Schmitt, *The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis*, 1 Harv. Nat'l Sec. J. 5, 26-27 (2010).

[191] Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, Wired, (July 11, 2011, 7), *available at* http://arstechnica.com/tech-policy/2011/07/how-digital-detectives-deciphered-stuxnet-the-most-menacing-malware-in-history/.

[192] *Id.*

[193] *Id.*

[194] *Id.*

zero-day exploits.[195] A few weeks later, VirusBlokAda employees reported the zero-day exploit and the malicious software to Microsoft, which later nicknamed the malicious code Stuxnet.[196]

As software engineers worldwide began dissecting Stuxnet's code, they discovered that it was designed to target specific industrial control software designed by Siemens, the very same software used by Iran's Natanz uranium enrichment facility.[197] Other aspects of the code, such as only targeting configurations containing 164 devices and references to a specific frequency, 1064Hz, seemed to confirm Natanz as the code's target.[198] Once Stuxnet found its target, it was designed to do two things: 1) periodically speed up and slow down certain motors connected to a frequency converter, and 2) trick monitoring systems by replacing status reports and shutting off system alarms.[199] This allowed Stuxnet to alter the normal operation of the industrial control system without raising operator awareness.[200]

Iranian centrifuges, used for enriching uranium, are based off of a Pakistani design and have a reputation for being extremely temperamental, "subject to periodic, random explosion."[201] In David Sanger's 2012 book, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, he says Stuxnet was a joint operation named "Olympic Games" between the United State and Israel.[202] Sanger says Olympic Games dated back to 2006 when President George W. Bush demanded a "third option" besides letting Iran develop a nuclear weapon or starting a war with Iran.[203] Stuxnet became that third option. According to Sanger, the goal was to capitalize on Iran's volatile centrifuge design by initiating a series of apparently random centrifuge failures, with the hope that Iranian authorities would lose faith in the design, the parts, and/or their engineers.[204]

One of Stuxnet's most intriguing aspects was its delivery. Natanz is a secure facility that is not connected to the Internet so its designers had to figure out a way to bridge the "air gap."[205] According to Symantec, Stuxnet was designed to spread

---

[195] Nicolas Falliere *et al.,* W32.Stuxnet Dossier, Version 1.4, Symantec Security Response 2 (Feb. 2011), *available at* http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf [hereinafter, Stuxnet Dossier].

[196] Zetter, *supra* note 191 (combining the file names .stub and MrxNet.sys from the software code).

[197] *Id.*

[198] *Id.*

[199] *Id.*

[200] *Id.*

[201] David E. Sanger, Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power 188-89 (2012).

[202] *Id.* at 188-91.

[203] Sanger, *supra* 201, at 188-191.

[204] *Id.* at 188.

[205] *Id.* at 195-96.

in several different ways, including through a vulnerability in removable drives with "auto-execution" software (thumb drives) and through local area networks (LANs) via a Windows Print Spooler vulnerability.[206] Stuxnet was designed to infect the computer systems of people with access to Natanz, who then might plug a laptop or a thumb drive into Natanz's closed network.[207] Additionally, each time Stuxnet infected a computer it would gather some basic information about the system, such as the machine's internal and external IP addresses, its name, details about the operating system, and whether it contained Siemens industrial control software.[208] Stuxnet would then report this information to a central command and control server attached to one or more domain names.[209] Symantec identified two of these command and control servers, one in Denmark and one in Malaysia.[210] The command and control servers could directly install updated versions of Stuxnet or other files on infected machines.[211] Additionally, infected computers continuously searched LANs or connected devices for updated versions of the code.[212] This meant that so long as Natanz insiders kept connecting thumb drives and laptops to both open and closed networks, updated versions of Stuxnet would eventually infect all targeted systems.

While Stuxnet eventually spread to 155 different countries[213] (as a result of an unintended programming mistake[214]), Symantec says it was initially targeted at five different organizations, all with a "presence in Iran".[215] Interestingly, the shortest time between the software compile time and initial infection time was 12 hours.[216] Such a short time between when the code was completed to when it infected a machine with an "Iranian presence" suggests that the code was initially delivered via the Internet as opposed to being covertly installed by hand.

2. Neutrality Analysis

While Stuxnet did not occur during an armed conflict and therefore did not directly raise any neutrality issues, it did prove an effective operational concept that will likely be used in future conflicts. As evidenced by the Estonia and Georgia

---

[206] Stuxnet Dossier, *supra* 195, at 2. Interestingly, the United States Department of Defense banned the use of thumb drives around this same time. *See* Noah Shachtman, *Under Worm Assault, Military Bans Disks, USB Drives*, WIRED (Nov. 19, 2008 3:12 PM), *available at* http://www.wired.com/dangerroom/2008/11/army-bans-usb-d/.

[207] Sanger, *supra* 201, at 196.

[208] Zetter, *supra* note 191.

[209] *Id.*

[210] Stuxnet Dossier, *supra* 195, at 21.

[211] Zetter, *supra* note 191.

[212] Stuxnet Dossier, *supra* 195, at 34.

[213] *Id.* at 6.

[214] Sanger, *supra* 201, at 204-205.

[215] Stuxnet Dossier, *supra* 195, at 7.

[216] *Id.*

examples, military leaders are seemingly learning the value of effective cyber operations and will likely incorporate them into future war plans. With Stuxnet's code now available for anyone to tinker with or modify, it is reasonable to assume that the next major international conflict will include malware similar to, or modeled after, Stuxnet. For example, industrial control systems, similar to the one used at Natanz, are found in petroleum refinement plants, chemical production plants, and electrical power generation and transmission plants.[217] It is fairly easy to imagine any of these plants as constituting a legitimate military target during a future armed conflict.

Using malware like Stuxnet in an armed conflict would raise at least two significant neutrality concerns: (1) the location of command and control servers and (2) delivery routes. The analysis of the command and control server issue is similar for a Stuxnet-type operation as it would be for a DoS attack but the arguments are stronger. Stuxnet used at least two different command and control servers, one in Malaysia and one in Denmark, but could have been updated throughout the operation to communicate with different command and control servers.[218] If Stuxnet had occurred during the course of an armed conflict, Malaysia and Denmark would have been in a difficult position. If Stuxnet was developed as a way to achieve effects comparable to attacking Natanz with conventional weapons,[219] it essentially substituted for conventional weapons. When military planners can use certain cyber capabilities and conventional weapons interchangeably, it defies logic to apply the neutrality rules to one and not the other.

With respect to Hague V, the analysis remains the same for the command and controls servers in the Stuxnet context as it does in the DoS attack context. The command and control servers in this scenario would be acting as virtual "wireless telegraphy stations" for the purpose of "communicating with belligerent forces" in violation of Article 3.[220] The Stuxnet command and control servers compiled data received from each infected computer[221] and presumably sent that data to Stuxnet's creators. Additionally, Stuxnet's creators likely used the command and control servers to push updated versions of the code out to infected computers.[222] In an armed conflict scenario, it would be difficult to argue that these command and control servers are not communicating with belligerent forces. Furthermore, if malware has the ability to shut down a power grid or cripple an oil refinery, a belligerent may be more likely to respond militarily once it discovers the threat. Such a response might include damaging or disabling any known command and control servers or other

---

[217] Systems and Network Analysis Center, National Security Agency, A Framework for Assessing and Improving the Security Posture of Industrial Control Systems (Version 1.1, Aug. 20, 2010), *available at* http://www.nsa.gov/ia/_files/ics/ics_fact_sheet.pdf.

[218] Stuxnet Dossier, *supra* note 195, at 21.

[219] Sanger, *supra* note 201, at 188-191.

[220] Hague V, *supra* note 10, art. 3.

[221] Stuxnet Dossier, *supra* note 195, at 21.

[222] Zetter, *supra* note 191.

vital network elements residing in that neutral state. As the likelihood of a military response against a neutral state's network components increases, so does the need to apply the law of neutrality in order to prevent the spread of conflict.

The other aspect of Stuxnet that raises potential neutrality issues concerns the specific delivery path or paths the malicious code travels. Does the law of neutrality prohibit malicious packets of information from traveling over the network infrastructure of a neutral state on the way to a belligerent target? Applying the law of neutrality to this particular scenario is problematic for two reasons. First, individual packets might not all take the same route and users may not be able to control the route.[223] Second, applicable neutrality rules are not likely needed in this situation to prevent the spread of conflict. Put another way, the fact that some packets travel over a neutral's network on the way to a belligerent is not likely to trigger any military action against the neutral's network. The Internet's redundant design means that any military action to shut down one particular route would not have much, or any, practical effect; the packets will just take a different route.[224] While not a perfect fit, this narrow situation should still fall under the scope of Hague V's telegraph exception.[225] The telegraph exception was largely based on practical limitations[226] that are especially applicable to controlling or monitoring the delivery routes of individual packets. Furthermore, using the roads analogy discussed earlier, it is more appropriate to view the telecommunications service provider as transporting the code in this scenario since it is the service provider who is directing the path, not the belligerent.

While it may not be appropriate to apply the neutrality rules to the delivery routes of individual packets in most cases, it is important to distinguish the situation where a belligerent uses a proxy in a neutral state. While belligerents may not be able to control the specific routes packets take, a belligerent *ensures* the packets go through a neutral state by using a proxy in that neutral state. A belligerent may use a proxy in a neutral state in order to make it appear as if the neutral state is supporting its effort or simply because the enemy may not scrutinize Internet traffic emanating from that neutral country in the same way it scrutinizes other Internet traffic. Either way, the deliberate use of proxy in a neutral state is likely an attempt to derive some form of military advantage from a neutral's territorial infrastructure and is prohibited.[227] This essentially collapses the neutrality analysis for the delivery of packets into an intent-based analysis, an approach often advocated.[228] Addition-

---

[223] *See* Boebert, *supra* note 120, at 41-42.

[224] *See id.* at 42.

[225] Hague V, *supra* note 10, art. 8.

[226] *See* Hague Reports, *supra* note 14, at 543.

[227] *See* Hague V, *supra* note 10, art. 1 ("The territory of neutral States is inviolable.").

[228] *See*, *e.g.*, Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 Harv. Int'l L.J. 179, 210-11 (2006); Jeffrey T.G. Kelsey, *Hacking into International Humanitarian Law: The Principles of Distinction and*

ally, while there may not be much practical value in taking military action against a neutral's network that is only carrying packets, "bricking"[229] a proxy may be an effective countermeasure. Neutral states should not become cyber battle grounds for belligerents, where the burden of collateral damage would rest entirely on the neutral state.

As in the Georgia example, attribution limitations will not bar military action. Attribution limitations are certainly relevant, especially in conducting a proportionality analysis, but the fact remains that objects which are being used to "make an effective contribution to military action" are military objects and may be attacked.[230] Every proxy computer in the chain would likely meet this definition and would therefore be subject to attack. For that matter, the cables that merely carry packets could also qualify as military, or dual-use, objects but the negligible military advantage to be gained by attacking them might be difficult to justify under a proportionality analysis.[231] As with the DoS attack scenario, it is technical attribution to a particular node/computer that triggers a belligerent's ability to take military action against that particular node/computer, regardless of whether the belligerent can further attribute the conduct to a person, organization, or government.[232]

## V. CONCLUSION

The neutrality rules are over a hundred years old and did not envision modern cyber capabilities but technological innovation in weaponry is nothing new. When cyber capabilities can viably substitute for conventional capabilities, whether they are damage-causing or damage-enabling capabilities, the neutrality rules must equally apply in order to preserve state sovereignty. Without applicable neutrality rules, belligerents will derive strategic advantages by purposely exploiting components of a neutral state's infrastructure. Allowing the cyber component of the battlefield to expand to neutral states erodes a neutral state's ability to stay out of a conflict. Belligerents do not seek symmetric responses. They constantly seek opportunities to overwhelm the enemy in the place and manner where they perceive an advantage. There is no guarantee that the cyber component of the battlefield could spread to neutral states without the conventional battlefield expanding there as well.

Attribution remains a challenge, especially when it comes to punishing belligerents who might choose to violate a neutral state's rights. Not only is technical attribution difficult but holding a state responsible also requires human attribution.

---

*Neutrality in the Age of Cyber Warfare*, 106 Mich. L. Rev. 1427, 1448-49 (2008).

[229] The term "bricking" refers to software or firmware changes that completely, and often permanently, disable a computer. *See* John Haubenreich, *The iPhone and the DMCA: Locking the Hands of Customers*, 61 Vand. L. Rev. 1507, 1538, n.201 (2008).

[230] Additional Protocol I, *supra* note 178, art. 52.

[231] *Id.* at art. 51.

[232] *See supra* notes 178-179 and accompanying text.

These attribution challenges may limit the deterrent value of applying the neutrality rules to cyber operations. However, as evidenced by the Mandiant report, large, prolonged cyber operations may be difficult to conceal indefinitely. Additionally, belligerents with sophisticated cyber capabilities may also rigorously monitor and control their own networks, strengthening attribution arguments based on Corfu Channel's rationale. Finally, while attribution certainly poses a problem in holding belligerents responsible for neutrality violations, it is less important when the neutrality rules are used to impose a duty on neutral states. Neutral states may not have the incentive to dedicate the resources necessary to monitor their own networks, but belligerents do. When a belligerent traces malicious cyber activity to components of a neutral state's infrastructure, it should be able to require the neutral state to take appropriate action if that state wants to remain neutral.

As with most areas of the law, technological advances create challenges. Sometimes the law is amended to explicitly deal with new technologies and sometimes the old law is interpreted to cover (or not cover) new technologies. When it comes to cyber capabilities and the law of neutrality, gaining international consensus to amend the law may not be possible and interpreting the law to not cover cyber operations threatens the entire institution of neutrality. By interpreting the neutrality rules with a focus on their purpose, states can usher respect for neutrality into twenty-first century warfare and continue to decide for themselves if and when to enter a conflict.

# WHEN THERE ARE NO ADVERSE EFFECTS: PROTECTING THE ENVIRONMENT FROM THE MISAPPLICATION OF NEPA

*Major Daniel J. White**



TABLE



* Maj Daniel J. White, Judge Advocate, United States Air Force (LL.M., with highest honors, Environmental Law, The George Washington University Law School (2013); J.D., West Virginia University College of Law (2000); B.A., Marshall University (1997)) is the Environmental Liaison Officer for Air Force Materiel Command, Wright-Patterson Air Force Base, Ohio. This paper was submitted in partial satisfaction of the requirements for the degree of Master of Laws in Environmental Law at The George Washington University Law School. The views expressed in this paper are solely those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense or U.S. Government.

## I. INTRODUCTION

In 2012, the U.S. Army undertook a project to preserve and restore over 8,600 acres of long-leaf pine forest at Fort Benning, Georgia.[1] This project of habitat conservation and environmental improvement demonstrates a remarkable transformation from what was occurring in the federal government forty-three years earlier. At that time, citing the examples of the Santa Barbara oil well blow out and controversies over an assured supply of clean water, Congress expressed concern that many agencies simply did not, or even could not under existing law, consider the effects to the environment before taking a particular action.[2] This resulted in President Richard Nixon signing the National Environmental Policy Act of 1969 (NEPA) into law, on January 1, 1970, as his first official act of the decade.[3] NEPA requires all federal agencies to take a "hard look" at the environmental impacts of any proposed federal action that has a significant impact on the environment. Now, however, projects such as the pine forest restoration at Fort Benning, which represent the fulfillment of the policy vision established by NEPA, are endangered by an overbroad interpretation of that Act.

At least one court has held that NEPA requires an Environmental Impact Statement (EIS) for projects with only *beneficial* significant impacts.[4] Requiring an EIS for these projects may well sound the "death knell" for agency actions that have only beneficial significant impacts.[5] Many actions by the government result in some kind of adverse effect[6] on the environment. Yet increasingly, the government is doing a better job of undertaking projects that embrace the national environmental policy to "create and maintain conditions under which man and nature can exist in productive harmony . . . ."[7] Actions that benefit the environment while causing no significant adverse impacts, pose a rarely considered question: Does a project with only beneficial significant environmental impacts require an agency to prepare an EIS?

---

[1] Office of the Sec'y of Def., Dep't of Def. Readiness and Environmental Protection Integration Program, *REPI in the News—2012*, *available at* http://www.repi.mil/InTheNews/2012.aspx (last visited August 5, 2013) [hereinafter REPI 2012].

[2] S. Rep. No. 91-296, at 8-9 (1969).

[3] Albert Ferlo et al., The NEPA Litigation Guide 1 (2d ed. 2012).

[4] *See* Nat'l Wildlife Fed'n v. Marsh, 721 F. 2d 767, 782-83 (11th Cir. 1983) (emphasis added); *see also infra* Part II.A.

[5] "There is also some feeling among agencies, project applicants, and even courts, that an EIS is the death knell of a project" *See* Ferlo et al., *supra* note 3, at 44 (citing Cronin v. United States Dep't of Agric., 919 F.2d 439, 443 (7th Cir. 1990)).

[6] CEQ definitions indicate that effect and impact are used synonymously throughout the NEPA implementing regulations. In this article, the two terms are also synonymous. *See* 40 C.F.R. § 1508.8 (2012).

[7] 42 U.S.C. § 4331 (2013).

Most recent cases have failed to answer the question of whether significant positive impacts on the environment trigger the need for an EIS.[8] However, looking back to the 1980s and 1990s, the Fifth and Eleventh Circuits appear to have answered this question in the affirmative, while the Sixth Circuit has concluded no EIS is required for impacts that are solely beneficial.[9] The Fifth Circuit has arguably backed away from this assertion, but was nevertheless relied upon by the Eleventh Circuit.[10] These three cases are all more than seventeen years old. While it is not surprising that very few NEPA lawsuits are brought by individuals seeking to prevent benefits to the environment, the argument is still raised regularly. Two district courts have addressed the argument in the two years preceding this article; the Ninth Circuit has discussed the issue in the last three years.[11] As agencies continue to take even more environmentally conscious actions, the argument may become increasingly relevant.

Since NEPA's enactment, there have been more and more governmental programs that are designed to find ways to enhance the environment while still allowing the government to complete its functions; for example, the longleaf pine restoration at Fort Benning. If NEPA requires that agencies prepare an EIS for projects with only beneficial significant impacts, agencies must comply with that requirement. However, because of the cost and delay associated with completing an EIS, agencies will be able to undertake fewer projects that *do* benefit the environment and may be deterred from undertaking such beneficial projects at all.

The cost of preparing an EIS, in both time and money, is a substantial burden. A 2003 report from the NEPA Task Force to the Council on Environmental Quality (CEQ) indicated an EIS at that time, took an average of one to six years to complete, and cost an average of $250,000 to $2,000,000.[12] In 2013 those costs are likely to be far higher, and agencies have substantially diminished resources as a result of the budget cuts under sequestration.[13] Accordingly, it is in an agency's

---

[8] *See, e.g.*, Humane Society v. Locke, 626 F.3d 1040, 1056 (9th Cir. 2010) (noting court has not decided question of whether an EIS is required for beneficial significant impacts); Coliseum Square Ass'n v. Jackson, 465 F.3d 215, 239 (5th Cir. 2006) (court has not arrived at an answer on whether an EIS is required for significant positive impacts).

[9] *See generally*, Friends of Fiery Gizzard v. Farmers Home Admin., 61 F.3d 501 (6th Cir. 1995). *Marsh*, 721 F.2d at 782-83.

[10] *See Coliseum Square Ass'n*, 465 F.3d at 239; *Marsh*, 721 F.2d at 782-83.

[11] *See* Oceana, Inc. v. Bryson, No. C-11-6257EMC, 2013 WL 1563675, at *24-25 (N.D. Cal. Apr. 13, 2013); S. Four Wheel Drive Ass'n v. United States Forest Service, No. 2:10CV15, 2012 WL 4106427, at *12-15 (W.D.N.C. Sept. 19, 2012); *Locke*, 626 F.3d at 1040.

[12] National Environmental Policy Act ("NEPA") Task Force, Council on Environmental Quality ("CEQ"), The NEPA Task Force Report to the Council on Environmental Quality: Modernizing NEPA Implementation 66 (2003), *available at* http://ceq.eh.doe.gov/ntf/report/finalreport.pdf [hereinafter Task Force Report].

[13] Letter from Jeffrey Zients, Deputy Director for Management of the Office of Management and Budget, to John A. Boehner, Speaker of the House of Representatives (Mar. 1, 2013) (on file with author), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/legislative_reports/fy13ombjcsequestrationreport.pdf.

best interest to avoid an EIS whenever possible. Courts have recognized that an EIS "is very costly and time-consuming to prepare and has been the kiss of death to many a federal project . . . ."[14] This has perhaps never been as true as it is now.

The possibility that courts could interpret NEPA to require an agency to prepare an EIS for a project with only beneficial significant impacts also creates a pathway for litigation from any group or individual wishing to block a project. NEPA documents have become a means, at least in part, to avoid litigation.[15] As a result, agencies may prepare lengthy, bulky impact statements primarily to avoid a fight in court.[16] If the litigation risk is large enough, an agency may be forced to prepare an EIS, even if they believe none would be required under a correct interpretation of NEPA, simply to ensure the project can proceed. In some instances, the timing of the project can be more important than the cost to an agency, and if litigation can be precluded, it may be possible to save a project that would otherwise have died in the courts.

The Department of Defense Readiness and Environmental Protection Integration program (REPI) [17] provides an example of the type of projects that are at risk. The purpose of this statute is to address the increasing problem of encroaching development around military bases.[18] In 2002, Congress authorized the various military departments to partner with other entities to acquire property and even enact conservation measures for lands surrounding military installations using REPI.[19] Military installations provide a concentration of personnel that business owners find attractive. Most bases have a number of restaurants and shops right outside their gates. In addition, the bases generally employ a large number of civilians in addition to the uniformed members. Hill Air Force Base, in Utah, claims to be the largest employer in the state, with more than 23,500 civilian, military and contractor personnel.[20] All of these people have to live somewhere and the demand for housing surrounding military installations is often fierce. However, all of the developments can negatively impact the mission of the base, as among other impacts, more people living close to a base complain about the noise of aircraft, more off base lighting affects night-time training and wildlife is pushed out of the newly developed areas around the base and onto the relatively open military installations.[21]

---

[14] *Cronin*, 919 F.2d at 443 (citing River Rd. Alliance, Inc. v. Corps of Eng'rs of United States Army, 764 F.2d 445, 449 (7th Cir. 1985)).

[15] Ferlo et al., *supra* note 3, at 3.

[16] *Id.*

[17] 10 U.S.C. § 2684a (2013).

[18] *See* Under Sec'y of Def. for Acquisition, Tech., and Logistics REPI 2013, 7th Annual Report to Congress 3 (2013) (discussion of issues pertaining to encroachment on military installations) [hereinafter REPI 2013].

[19] 10 U.S.C. § 2684a(d)(2).

[20] *See* Hill Air Force Base, OO-ALC Mission, *available at* http://www.hill.af.mil/main/welcome.asp (last visited June 21, 2013).

[21] *See* REPI 2013, *supra* note 18, at 2.

REPI is designed to provide a tool that will help to prevent or remedy the some of the problems created by encroaching development. The most common use of REPI is to acquire some sort of easement that will prevent development of the land and leave it in its natural, or at least, its current state.[22] However, REPI projects do occasionally include enhancements to the environment. For example, Fort Benning is using the REPI program to benefit 8,600 acres of longleaf pine forest.[23] This REPI project goes beyond merely preserving the forest in its current state; instead, REPI partners have actually altered the current landscape by restoring the native forest and replanting native species of grasses and longleaf pine, creating habitat for the endangered gopher tortoise and red-cockaded woodpecker.[24] Arguably, this project could have a significant, beneficial impact on the environment.

In 2012, there were a total of 677 REPI projects reported.[25] Total REPI funding was just over $215 million.[26] This represents approximately $318,000 per project on average. If the cheapest environmental impact statements reported in 2003 were $250,000 and some more expensive impact statements cost in the millions, it is easy to see how funding for projects could quickly become exhausted by NEPA paperwork, resulting in a dramatic reduction in the number of REPI projects that the DoD could accomplish. Obviously, the size and scope of the projects differ and not all REPI projects would require an EIS under any standard, since some would have no impact on the environment at all. Still, the cost of an EIS could make the more environmentally beneficial projects, such as the one at Fort Benning, untenable. Interpreting NEPA to require an EIS for beneficial significant impacts, merely to explain how the government is going to help the environment, would result in the waste of at least $250,000, and potentially millions of dollars. Worse, it would be contrary to the declared purpose of NEPA for the statute to be used to prevent such projects, either through litigation or because of excessive cost.

This article will supplement current literature, explaining that despite some cases to the contrary, requiring an EIS for beneficial significant impacts is inconsistent with the purpose of NEPA and with current NEPA implementation. The precise definition of what constitutes a "significant impact" is unclear in both NEPA and the implementing regulations promulgated by CEQ. However, this ambiguity can be resolved by deferring to agency interpretation of agency promulgated NEPA regulations. To that end, Part II of this article will provide a background overview of NEPA and its requirements. Part III will examine the case law that has interpreted

---

[22] U.S. Dep't of Def., Partner's Guide to the Department of Defense's Readiness and Environmental Protection Initiative *(REPI)*, at 9, *available at* http://www.repi.mil/Documents/Primers/Primer_REPI.pdf.

[23] REPI 2012, *supra* note 1.

[24] Charles Seabrook, *Wildlife and the Military Benefit from Forest Restoration*, Atlanta J.& Const, Dec. 7, 2012, *available at* http://www.ajc.com/news/lifestyles/wildlife-and-the-military-benefit-from-forest-rest/nTNN7/.

[25] *See* REPI 2013, *supra* note 18, at 3.

[26] *See* REPI 2013, *supra* note 18, at 3.

the requirement to prepare an EIS for beneficial significant impacts, and analyze NEPA's legislative history and implementing regulations. Part IV will then look at the possibility of agencies relying on their own agency promulgated regulations for a solution. The deference given to an agency's interpretation of its own regulations may be the strongest defense to an argument that an EIS is required for projects with solely beneficial impacts.

## II. BACKGROUND AND OVERVIEW OF NEPA REQUIREMENTS

In the 1960s, there were several proposals before Congress suggesting the need for a national environmental policy and proposing an executive council to address growing concern over the environment.[27] The Senate committee report, addressing the proposed National Environmental Policy Act, spoke of the need for environmental legislation, noting:

> There is no general agreement as to how critical the Nation's present environmental situation has become. Some respected scholars insist that a number of crises already exist. Others maintain that there is yet time to prevent them. There is nearly unanimous agreement, however, that action is needed and that, at least in some instances, dangerous conditions exist.[28]

NEPA was Congress' groundbreaking response and has been heralded as an environmental Magna Carta for the United States.[29] The Act did three basic things. First, it declared a national environmental policy.[30] Second, it included a provision that requires agencies to complete what has become known as the environmental impact statement prior to undertaking any major federal action significantly affecting the quality of the human environment.[31] Finally, it created a CEQ, which among other duties, was to advise the President on environmental matters and review the programs of the federal government in light of the new environmental policy.[32]

CEQ was set up as a three member council charged with advising the President and helping to "formulate and recommend national policies to promote the improvement of the quality of the environment."[33] In addition, CEQ has been recognized as the arbiter of disagreements between federal agencies in implementing

---

[27] Linda Luther, Cong. Research Serv., RL 33152, The National Environmental Policy Act (NEPA): Background and Implementation 2-3 (2011).

[28] S. Rep. No. 91-269, at 13.

[29] Daniel R. Mandelker, NEPA Law and Litigation: The National Environmental Policy Act § 1:1 (2012).

[30] 42 U.S.C. § 4331.

[31] *Id.* § 4332 (2013).

[32] *Id.* §§ 4342-44 (2013).

[33] *Id.* § 4342.

NEPA and the nation's environmental policy.[34] Perhaps most important, however, was that in 1970, President Nixon issued an executive order directing CEQ to issue regulations for the various federal agencies to direct their compliance with the procedural portions of NEPA.[35] As a result, CEQ replaced their initial guidelines with new regulations in 1978, which have been subsequently interpreted as binding on all federal agencies.[36] These regulations will be discussed in detail in Part III.D.

NEPA's declared environmental policy has remained unchanged for 44 years. Congress has stated that it is national policy to:

> [U]se all practicable means and measures, including financial and technical assistance, in a manner calculated to foster and promote the general welfare, to create and maintain conditions under which man and nature can exist in productive harmony, and fulfill the social, economic, and other requirements of present and future generations of Americans.[37]

Agencies must comply with NEPA and this policy, "to the fullest extent possible."[38] NEPA also contains an action forcing provision which requires that for every legislative proposal or "other major Federal actions significantly affecting the quality of the human environment . . . ,"[39] agencies prepare a detailed statement, which explains:

> (i) the environmental impact of the proposed action,
>
> (ii) any adverse environmental effects which cannot be avoided should the proposal be implemented,
>
> (iii) alternatives to the proposed action,
>
> (iv) the relationship between local short-term uses of man's environment and the maintenance and enhancement of long-term productivity, and
>
> (v) any irreversible and irretrievable commitments of resources which would be involved in the proposed action should it be implemented.[40]

This detailed statement is what has become known as EIS.

---

[34] *See* 42 U.S.C. § 4344(3); 42 U.S.C. § 4332(C); 42 U.S.C. § 7609(b) (2013); *see also* 40 C.F.R. § 1504.1 (1979).

[35] Exec. Order No. 11,514, 3 C.F.R. § 123 (1978).

[36] *See* Andrus v. Sierra Club, 442 U.S. 347, 357 (1979).

[37] 42 U.S.C. § 4331(a).

[38] *Id.* § 4332.

[39] *Id.* § 4332(C).

[40] 42 U.S.C. § 4332(C)(i)-(v).

Courts have recognized two main reasons for preparing an EIS. First, Section 102 requires agencies to use a systematic, interdisciplinary approach to planning and decision-making, which considers environmental values.[41] Presumably, decision-makers will utilize the EIS to make, if not more environmentally friendly decisions, at least more informed decisions. The second recognized purpose of the EIS is not so easily found in the text of NEPA. Nevertheless, the United States Supreme Court has recognized informing the public that the agency has considered environmental concerns is one of NEPA's "twin aims."[42] Public participation, while not spelled out strictly in the Act itself, is required under CEQ regulations.[43]

These regulations create three tiers of NEPA analysis. For projects that will have a significant impact on the human environment, the agency must prepare an EIS.[44] This is the most comprehensive document, and, as noted above, the most expensive option for NEPA compliance. It is also the only option that actually appears in the Act itself.[45] Since the promulgated regulations went into effect, and due to the time and expense of creating the statement, there has been a marked trend away from preparing a full EIS. In 1973, approximately 2,000 EISs were filed with the Environmental Protection Agency (EPA).[46] By 1979, that number had fallen to 1,273.[47] Ten years on, a staggering reduction had occurred, only 370 EISs were filed in 1989.[48] That number has since fluctuated, but hovers around 500, with a total of 450 EISs filed in 2009, the most recent year for which CEQ has made data available.[49] Conversely, CEQ reported by 1993, over 50,000 environmental assessments were being prepared annually.[50]

The Environmental Assessment (EA) is a shorter report that represents the second tier of environmental analysis under CEQ's NEPA regulations. Some agencies had adopted the approach of drafting an EA to document their finding that no EIS was required, even before CEQ's biding regulations.[51] However, the uniform distinction between an EA and an EIS, and its mandatory use, is a creation of those

---

[41] *Id.* § 4332(A)-(B).

[42] Baltimore Gas & Elec. Co. v. Natural Res. Def. Council, Inc., 462 U.S. 87, 97 (1983).

[43] *See* 40 C.F.R § 1503 (2012).

[44] *See* 42 U.S.C. § 4332(C); 40 C.F.R. §1501 (2012).

[45] 42 U.S.C. § 4332(C).

[46] CEQ, Environmental Quality 25th Anniversary Report, 51 (1997), *available at* http://ceq.hss.doe.gov/nepa/reports/1994-95/25th_ann.pdf [hereinafter CEQ 25th Anniv. Report].

[47] CEQ 25th Anniv. Report, *supra* note 46, at 534.

[48] *Id.*

[49] *Id.*; CEQ, Environmental Quality, Calendar Year 2009 Filed EISs, *available at* http://ceq.hss.doe.gov/nepa/Calendar_Year_2009_Filed_EISs.pdf.

[50] CEQ 25th Anniv. Report, *supra* note 46, at 51.

[51] *See* Hanley v. Kleindienst, 471 F.2d 823 (2d Cir. 1972) (discussing GSA-prepared environmental assessment to show EIS was unwarranted).

regulations.[52] An EA is designed to be used when the agency is unclear if the action will result in significant impacts or if it is the type of action that normally results in no significant environmental impacts but has not been categorically excluded.[53]

In addition to creating the tiers of environmental analysis, CEQ regulations required agencies to promulgate supplemental regulations.[54] These supplemental regulations required agencies to identify classes of actions, and criteria for classes of actions, that normally require an EIS or an EA.[55] Agencies also were required to identify classes of action that did not normally require an EA or an EIS.[56] These actions would qualify for the third tier of analysis, a Categorical Exclusion (CATEX).[57]

Categorical exclusions represent an entirely different type of analysis. If an agency determines an action falls under a CATEX, further analysis (under an EA or an EIS) is unnecessary and the agency merely records the applicable CATEX.[58] CEQ reports this has become the most common way for agencies to comply with NEPA.[59] Categorical exclusions must be promulgated by agencies as formal regulations, with public notice and comment periods, and must be approved by CEQ prior to an agency availing themselves of their use.[60] An example of a CATEX from the U.S. Army Corps of Engineers (hereinafter "Corps"), would be the construction of a small floating private pier.[61] This is an action, which while subject to the Corps' regulation, has been determined not to produce any significant environmental impacts. Accordingly, the Corps can determine a CATEX applies, and no EA or EIS is required.

Under the CEQ regulations, any time an agency undertakes a major federal action which is not exempt from NEPA, there must be some form of NEPA compliance. The agency must either prepare an EA, an EIS, or determine if a CATEX applies. Both the EA and the EIS are released for public review and comment.[62] A CATEX generally represents a more routine project of little interest. The CEQ regulations do not specify public comment on such an activity. To achieve NEPA compliance, courts have only required that agencies create a short document, made

---

[52] *See* 40 C.F.R. § 1501.

[53] *Id.*

[54] *See* 40 C.F.R. § 1507 (2012).

[55] *See* 40 C.F.R. § 1507.3.

[56] *Id.*

[57] *Id.*

[58] *See* 40 C.F.R. § 1508.4 (2012).

[59] CEQ, *CEQ issued NEPA Guidance on Categorical Exclusions on November 23, 2010*, National Environmental Policy Act, *available on www.nepa.gov at* http://ceq.hss.doe.gov/current_developments/new_ceq_nepa_guidance.html#exclusions (last visited Aug. 5, 2013).

[60] 40 C.F.R. § 1507.3.

[61] 33 C.F.R. § 325 app. B § 6(a)(1) (2012).

[62] *See* 40 C.F.R. § 1501.4; 40 C.F.R. § 1506.6 (2012).

contemporaneously with the decision to undertake the activity, indicating that environmental effects have been considered and a CATEX has been determined to apply.[63]

All major actions of a federal agency that are not exempted from NEPA must fall into one of the three categories: EIS, EA, or CATEX. If an agency undertakes an action that is not categorically excluded and is expected to have no significant environmental impacts, the agency must prepare an EA and make a Finding of No Significant Impact (FONSI).[64] If the action will have significant environmental impacts, then the agency must prepare an EIS.[65] The question, therefore, is what is considered to be a significant impact?

In many cases, language from the CEQ and the courts has assumed, without explicitly stating, that significant environmental impacts is synonymous with adverse environmental impacts.[66] For example, at least one early case indicated that in deciding whether an action has a "significant" effect, the agency must review the adverse environmental effects the action will cause.[67] Early CEQ guidance also provided that to have a significant effect, the agency action would have to adversely impact the environment.[68] The 1978 NEPA regulations were not as clear; however, and the circuits remain split as to whether agency actions that will have only beneficial significant impacts should be analyzed under an EA or an EIS.

## III. AN EIS SHOULD NOT BE REQUIRED FOR BENEFICIAL IMPACTS

Although NEPA can be read to require an EIS for beneficial significant impacts to the environment, such a reading would be incorrect and makes little sense. Nevertheless, some commentators have embraced this interpretation, though there is little basis in statute or case law for their opinion.[69] At least one circuit has also held that an EIS would be required for beneficial significant impacts.[70] Such an approach ignores the spirit of NEPA's implementing regulations and at times, as in the case of REPI projects discussed above, would produce results that are contrary to the purpose of the act itself.

---

[63] *See, e.g.*, California v. Norton, 311 F.3d. 1162, 1176 (9th Cir. 2002).

[64] 40 C.F.R. § 1501.4.

[65] *Id.*

[66] *See infra* Part II.D.

[67] *See Hanley*, 471 F.2d at 830-31.

[68] *See* Preparation of Environmental Impact Statements: Guidelines, 38 Fed. Reg. 20,550-20,562, 20,551-20,552 (Aug. 1, 1973) (to be codified at 40 C.F.R. pt. 1500.6).

[69] *See e.g.*, Neal McAliley, *NEPA and Assessment of Greenhouse Gas Emissions*, 41 Envtl. L. Rep. News & Analysis, 10197, 10198-199 (2011).

[70] *Marsh*, 721 F.2d at 782-84.

To explain why requiring an EIS for projects with only beneficial significant impacts is incorrect, this article will address the current circuit split and what seems to be the origin of the beneficial EIS theory. Part III.C will look to the legislative history of NEPA and analyze the purpose of the statute. Next, Part III.D will examine the CEQ regulations and how they have been interpreted since promulgation in 1978. Finally, Part III.E will look to the doctrine of functional equivalence and some of the exclusions Congress has granted for statutory programs, which demonstrate that a beneficial EIS requirement is inconsistent with the courts' interpretations of NEPA and arguably the interpretation of Congress.

A. The Origin of the Beneficial EIS and the Circuit Split

In 2010, the Ninth Circuit recognized a split in the circuit courts as to whether an agency was required to prepare an EIS for projects with significant, though only beneficial, environmental impacts.[71] In spite of this, at least one author has argued that there is in fact no split in the circuits,[72] and that in accordance with the Sixth Circuit, agencies are not required to prepare an EIS under current law for beneficial significant impacts.[73] This argument makes some sense, particularly in light of a Fifth Circuit case, in which the court distanced itself from an apparent holding that an EIS was required for projects with only beneficial significant impacts.[74] However, ultimately the claim that there is no circuit split cannot be supported.

The Eleventh Circuit has held that a Supplemental EIS (SEIS) is required for changes in a project that produce only beneficial significant impacts.[75] An argument that this decision is distinguishable because it deals only with the preparation of an SEIS, as opposed to an EIS, fails because the Eleventh Circuit has also held that "[t]he standard for determining when an SEIS is required is 'essentially the same' as the standard for determining when an EIS is required." [76] If the "post-[original EIS] changes in the [project] will have a 'significant' impact on the environment that has not previously been covered by the [original] EIS, [an SEIS] is necessary."[77] If the standard is essentially the same, it is impossible to separate the standard of when to prepare an SEIS from the standard of when an EIS is required. It is in fact the same standard. In the Eleventh Circuit, therefore, the requirement for an EIS

[71] *Locke*, 626 F.3d at 1056.

[72] *See* Shaun A. Goho, *NEPA and the "Beneficial Impact" EIS*, 36 WM. & MARY ENVTL. L. & POL'Y REV. 367, 375-76 (2012)(arguing there is no circuit split, as the Fifth and Eleventh Circuits do not address preparation of an EIS, but only when a supplemental EIS is required).

[73] *Friends of Fiery Gizzard*, 61 F.3d at 506.

[74] *Coliseum Square Ass'n*, 465 F.3d at 239 (court has not arrived at answer as to whether an EIS is required for significant positive impacts).

[75] *See Marsh*, 721 F.2d at 782-84.

[76] Sierra Club v. U.S. Army Corps of Eng'rs 295 F.3d 1209, 1215-16 (11th Cir. 2002) (citing Envtl. Def. Fund v. Marsh, 651 F.2d 983, 991 (5th Cir. Unit A July 1981)).

[77] *Sierra Club*, 295 F.3d at 1216 (internal citations omitted).

would be triggered any time there is a significant environmental impact, whether beneficial or adverse.[78]

1. The Seeming Origin of the Beneficial Impact EIS Requirement

The story of this holding and the resulting circuit split does not begin in the Eleventh Circuit, but rather in the Fifth Circuit in 1973.[79] In *Hiram Clarke Civic Club, Inc. v. Lynn*, (hereinafter "*Hiram Clarke*"), the Department of Housing and Urban Development (HUD) guaranteed and subsidized a loan for the construction of an apartment complex.[80] Given the extent of federal involvement in the project, NEPA applied and HUD evaluated the project under agency regulations and determined that no EIS was required, as there were no significant adverse impacts.[81] Project opponents challenged this decision, in part, on the grounds that an EIS should be required for *any* significant impact, even beneficial impacts.[82] The court never reached this issue, upholding the ruling for the government after finding the district court had conducted a full evidentiary hearing and explored the controlling factors.[83] The court did not do this, however, without making some remarks that would prove problematic. In discussing the appellants' argument that an EIS should be required because of beneficial significant impacts, the court provided language that would be relied upon in future decisions:

> We think this contention raises serious questions about the adequacy of the investigatory basis underlying the HUD decision not to file an environmental impact statement. A close reading of Section 102(2)(C) in its entirety discloses that Congress was not only concerned with just adverse effects but with *all* potential environmental effects that affect the quality of the human environment.[84]

CEQ regulations at this time were only guidance and agencies were not bound by them as matter of law.[85] Since the guidance was not mandatory, it also did not represent a uniform approach by all agencies. More importantly, this guidance was substantially different than the regulations CEQ eventually promulgated in 1978 and appears to have lent more weight to the argument for a beneficial EIS requirement than would later regulations. There were two important aspects of this initial guidance that explain the court's rationale. First, the guidance at issue

---

[78] *Marsh*, 721 F.2d at 783-84.

[79] *See* Hiram Clarke Civic Club, Inc. v. Lynn, 476 F.2d 421 (5th Cir. 1973).

[80] *Hiram Clarke Civic Club, Inc.*, 476 F.2d at 422-23.

[81] *Id.* at 426.

[82] *Hiram Clarke Civic Club, Inc*, 476 F.2d at 426 (emphasis added).

[83] *Id.* at 427.

[84] *Id.* (emphasis added).

[85] *See* Statements on Proposed Federal Actions Affecting the Environment, 36 Fed. Reg. 7724-7729 (Apr. 23, 1971).

when the case was decided was published in 1971 and did not provide an option to produce an EA as opposed to an EIS, but simply referred to a single environmental statement.[86] Therefore, the court may have concluded if any kind of NEPA compliance was required, there was only one option—the EIS mentioned in the statute.

Second, under CEQ's 1971 guidance, in effect at the time this case was decided, the concept of significant effects on the environment was much broader. Appellants relied on guideline 5(c), which stated: "Section 101(b) of the Act indicates the broad range of aspects of the environment to be surveyed in any assessment of significant effect."[87] Section 101(b) of NEPA provides a list of objectives by which federal programs could implement the national environmental policy. These are:

> (1) fulfill the responsibilities of each generation as trustee of the environment for succeeding generations;
>
> (2) assure for all Americans safe, healthful, productive, and esthetically and culturally pleasing surroundings;
>
> (3) attain the widest range of beneficial uses of the environment without degradation, risk to health or safety, or other undesirable and unintended consequences;
>
> (4) preserve important historic, cultural, and natural aspects of our national heritage, and maintain, wherever possible, an environment which supports diversity and variety of individual choice;
>
> (5) achieve a balance between population and resource use which will permit high standards of living and a wide sharing of life's amenities; and
>
> (6) enhance the quality of renewable resources and approach the maximum attainable recycling of depletable resources.[88]

Using these goals to analyze impacts, it is easy to see how the Fifth Circuit might reach the conclusion that NEPA's significant impact requirement might include beneficial impacts, especially when the EA was not an option. After all, if an agency is supposed to survey impacts to "preserve important historic, cultural, and natural aspects of our national heritage, and maintain, wherever possible, an environment which supports diversity and variety of individual choice,"[89] it would seem that beneficial impacts would have to be part of the analysis. The same is true for several

---

[86] *Id.*

[87] *Hiram Clarke Civic Club, Inc.*, 476 F.2d at 426 (citing 36 Fed. Reg. at 7725 (1971)).

[88] 42 U.S.C. § 4331(b)(1)-(6).

[89] 42 U.S.C. § 4331(b)(4).

of the other objectives. In this case, given the court's focus on the guideline pointing to section 101(b), its reasoning can be understood.

This was not the correct approach, however, even under the early guidelines. The court only looked at part of section 5(c) of the 1971 guidance, the portion that addressed what effects "needed to be surveyed in any assessment of significant effect."[90] The list of goals did not define what a significant effect was, it merely provided a background for what would be affected in determining if an effect did rise to the level of significance. Ultimately, the analysis from the court in this case regarding the necessity to produce an EIS for beneficial effects was incomplete. This is understandable, as it was dicta and not a large portion of the analysis of the case, since the court repeatedly indicated that failing to comply with the CEQ guidance did not violate any substantive duty.[91] Had a more thorough analysis been performed, it is possible the court may have reached the conclusion that beneficial impacts did not require an EIS. Nevertheless, given the portion of the guidance the court chose to rely upon, the court's concern with beneficial effects is understandable.

When CEQ promulgated new regulations in 1978, they provided substantially more information as to what might be considered a significant impact. These new regulations were binding on federal agencies[92] and no longer pointed to Section 101(b) of NEPA as a guide for any measure of significant effects. CEQ instead provided a rather complex definition of "Significantly," that "requires consideration of both context and intensity."[93] Under the new regulations, context meant that analysis should focus on the affected population groups or regions of the action.[94] In other words, an agency should ask whether the action affects only local populations or interests or if it has more far reaching consequences. Significance could therefore change under the new regulations, depending on the locales and groups affected.[95] Intensity "refers to the severity of the impact."[96] The regulations then provide a list of ten factors to consider in evaluating intensity. The new factors are much more focused on specific effects, rather than relying on policy declarations. Had *Hiram Clarke* been decided under these regulations, it is entirely possible the court would have addressed the discussion of an EIS for impacts that are solely beneficial.

---

[90] Statements on Proposed Federal Actions Affecting the Environment, 36 Fed. Reg. at 7725.

[91] *See generally Hiram Clarke Civic Club, Inc.*, 476 F.2d at 426-27.

[92] *See Andrus*, 442 U.S. at 357.

[93] 40 C.F.R. § 1508.27.

[94] *Id.*

[95] 40 C.F.R. § 1508.27.

[96] *Id.*

2. The Fifth Circuit

In 1981, this issue again came up in the Fifth Circuit in relation to the Tennessee-Tombigbee Waterway (TTW).[97] The TTW was a project of the U.S. Army Corps of Engineers to create a canal designed to connect the Tennessee River in the north, with the Black Warrior-Tombigbee Waterway in the south.[98] The TTW created a continuous route between the upper Ohio and Mississippi valleys and the Gulf of Mexico.[99] The project had been around in one form or another since it was first authorized by Congress in 1946, and the initial EIS for the project was prepared and filed in 1971.[100] The sufficiency of that EIS was challenged, but upheld by the Fifth Circuit in 1974.[101] Subsequent to that decision, as one might expect in a project that spanned 253 miles and cost more than $2 billion, there were several design changes.[102] The project shifted on one section, from the design of a standard "perched canal" using artificial levees on both sides, to a "chain of lakes" design, with levees on only one side and flooding to the natural hill barrier on the other.[103] On another section, the Corps decided to straighten the Tombigbee River, by digging out cutoffs to connect bends.[104] The project changes also created an additional nine million cubic yards of spoil that would require disposal.[105] In spite of these changes, the Corps maintained that no SEIS was necessary.[106]

To demonstrate compliance with NEPA, the Corps cited to agency regulations that permitted the Corps to rely on a more informal document "[w]henever it is necessary only to clarify or amplify a point of concern raised after the final environmental statement was filed with CEQ [Council on Environmental Quality] (and such point of concern was considered in making the initial decision) . . . ."[107] The court noted that by treating all post 1971 changes as informal under this section, the Corps had filed 18 volumes of informal supplemental reports as opposed to performing a formal SEIS.[108] This led to the Fifth Circuit laying out for the first time the legal standard for when an SEIS is required. Its holding, in pertinent part, stated:

> We therefore hold that NEPA does require the supplementation of an EIS when subsequent project changes can, in qualitative or quan-

---

[97] *See Marsh*, 651 F.2d at 983.

[98] *Marsh*, 651 F.2d at 986.

[99] *Id.*

[100] *Id.* at 987.

[101] *See* Envtl. Def. Fund, Inc. v. Corps of Eng'rs, 492 F.2d 1123, 1139-40 (5th Cir. 1974).

[102] *Marsh*, 651 F.2d at 986-90.

[103] *Id.* at 987.

[104] *Id.* at 987-88.

[105] *Id.* at 988.

[106] *Id.*

[107] *Marsh*, 651 F.2d at 989 (citing 33 C.F.R. § 209.410(g)(3) (1981)).

[108] *Marsh*, 651 F.2d at 989.

> titative terms, be classified as "major Federal actions significantly affecting the quality of the human environment." 42 U.S.C. § 4332. The standard of the need for an original EIS and of the need for a supplement to that EIS, therefore, is essentially the same; it merely focuses the inquiry on a different body of information to evaluate the "significance" of the environmental impact.[109]

The appellants pointed to several impacts that they believed were significant and had not been considered in the original EIS, as they resulted from the project changes. These included: increased traffic on the canal, which would mean increased turbidity; bank sloughing and pollution; increased loss of wildlife habitat; and the possible creation of thousands of acres of stagnant, eutrophic water.[110] The court appeared to believe that these impacts could result from the changed design and that they remained unaddressed in the original EIS.[111] If that were true, it would have been reasonable for the court to conclude that these new adverse impacts required the Corps to go back and prepare a formal SEIS. But the court's analysis was not based entirely on the new adverse effects the changes may have caused.

Relying heavily on *Hiram Clarke*, the court also pointed out potentially beneficial effects, and appeared to include these as impacts that could necessitate an SEIS.[112] At one point the court noted:

> [M]erely because some of the new land acquisitions may have been intended to "mitigate environmental impact" does not shield those acquisitions from review under NEPA and the Corps' own regulations. The proper question is not the intent behind the actions, but the significance of the new environmental impacts. And even if the Corps was correct in deciding that the new land use will be beneficial in impact, a beneficial impact must nevertheless be discussed in an EIS, so long as it is significant. NEPA is concerned with all significant environmental effects, not merely adverse ones.[113]

This language seems to come straight from *Hiram Clarke*, which would make the analysis reliant on regulatory guidance that no longer existed. When the Corps attempted to argue that an SEIS was not required, as there were no new adverse impacts, the court "[found] no solid evidence that the Corps ha[d] ever asked the right question . . . ."[114] Instead, in response to the Corps' assertion that there were no new adverse impacts, the court again cited to *Hiram Clarke*, concluding:

---

[109] *Id.* at 991.

[110] *Id.* at 992-95.

[111] *Id.*

[112] *Marsh*, 651 F.2d at 994.

[113] *Id.* at 993 (citing *Hiram Clarke Civic Club, Inc.*, 476 F.2d at 426-27).

[114] *Marsh*, 651 F.2d at 996.

"[it] is simply the wrong standard. NEPA requires the discussion of all significant environmental impacts, not just adverse ones."[115] According to the Fifth Circuit, the "material" question before the court was "does the design have any significant new environmental impacts, whether beneficial or harmful?"[116] Other than citing to *Hiram Clarke*, the court provided no analysis for how it reached what seemed to be the conclusion that the requirement to produce an EIS could be triggered by a project with only *beneficial* significant impacts.

The court's reliance on *Hiram Clarke* ignored the new regulations that were promulgated in 1978 by CEQ. These regulations, as noted above, provided substantial guidance on how significant impacts should be defined[117] and were binding on the Corps.[118] Furthermore, the U.S. Supreme Court had already determined that these regulations were entitled to substantial deference.[119] Even if one were to accept that the new regulations might define significant impacts as including beneficial impacts, there is no indication that the court looked to them for any guidance on the issue. The only reference to CEQ regulations was in determining the standard for when an SEIS might be required.[120] Accordingly, the court's analysis in this regard is highly suspect, if not outright wrong. This may be part of the reason why the Fifth Circuit appeared to distance itself from this conclusion in its 2006 decision.

In *Coliseum Square Association, Inc. v. Jackson*,[121] (hereinafter "*Coliseum Square*"), opponents to a HUD-financed building project argued that an EIS was required "even though the project [had] no significant negative environmental effects, so long as it [had] significant positive environmental effects."[122] In responding to that argument, the Court referenced both *Hiram Clarke* and *Environmental Defense Fund v. Marsh*.[123] It noted that, while the court identified the issue in *Hiram Clarke*, it failed to actually provide a ruling on the issue.[124] The Court then distinguished *Environmental Defense Fund v. Marsh*, characterizing the holding in that case as only determining whether an EIS needs to discuss positive impacts.[125] Appellants likely were not expecting such a narrow interpretation from the Court, given the language cited above. Nevertheless, despite the plain language in *Environmental*

---

[115] *Id.* at 997 (citing *Hiram Clarke Civic Club, Inc.*, 476 F.2d at 426-27).

[116] *Marsh*, 651 F.2d at 994.

[117] 40 C.F.R. § 1508.27.

[118] *See Andrus*, 442 U.S. at 357.

[119] *Id.*

[120] *Marsh*, 651 F.2d at 988-92. Footnotes 4 and 10 reference the CEQ regulations in comparison to the Corps' agency regulations.

[121] 465 F.3d 215 (5th Cir. 2006).

[122] *Coliseum Square Ass'n*, 465 F.3d at 239.

[123] *Id.*

[124] *Coliseum Square Ass'n*, 465 F.3d at 239 (citing *Hiram Clarke Civic Club, Inc.*, 476 F.2d at 426-27).

[125] *Coliseum Square Ass'n*, 465 F.3d at 239 (citing *Marsh*, 651 F.2d at 993).

*Defense Fund v. Marsh*, the Fifth Circuit distanced itself from an affirmative holding that an EIS or SEIS is required for projects with only beneficial impacts and refused to provide a definitive answer to the question in *Coliseum Square*.[126]

3. The Eleventh Circuit

In October 1981, a split in the Fifth Circuit resulted in the creation of the Eleventh Circuit.[127] On November 3, 1981, the newly-formed Eleventh Circuit published its first opinion, holding, in pertinent part:

> [D]ecisions of the United States Court of Appeals for the Fifth Circuit (the "former Fifth" or the "old Fifth"), as that court existed on September 30, 1981, handed down by that court prior to the close of business on that date, shall be binding as precedent in the Eleventh Circuit . . . .[128]

The Fifth Circuit published its *Environmental Defense Fund v. Marsh* decision on July 13, 1981, and, as such, was binding precedent on the newly-formed Eleventh Circuit.[129] In 1983, when the Eleventh Circuit was asked to rule on a supplemental EIS for changes to a project with only beneficial impacts, it naturally turned to the Fifth Circuit decision of a few years earlier in *Environmental Defense Fund v. Marsh*.[130]

In *National Wildlife Federation v. Marsh*,[131] appellants challenged the EIS for a HUD-financed community improvement project and implemented by the city of Alma.[132] The EIS analyzed several improvement projects resulting from Alma's selection for participation in the Model Cities Program in 1968.[133] One of the projects was the construction of a reservoir on Hurricane Creek that became known as Lake Alma.[134] A final EIS was filed in 1976, but EPA and the Fish and Wildlife Service (FWS) objected to the project because of environmental concerns.[135] Due to these concerns, HUD refused to release funds for the project.[136] Ultimately, as part of

---

[126] *Coliseum Square Ass'n*, 465 F.3d at 239.

[127] Fifth Circuit Court of Appeals Reorganization Act of 1980, P.L. 96-452, 94 Stat. 1994 (1980).

[128] Bonner v. City of Prichard, Alabama, 661 F.2d 1206, 1207 (11th Cir. 1981).

[129] *See generally*, *Marsh*, 651 F.2d at 983.

[130] *See Marsh*, 721 F.2d at 782-83.

[131] 721 F.2d 767 (11th Cir. 1983).

[132] *Id.* at 771.

[133] *Id.* at 770.

[134] *Id.*

[135] *Id.* at 771.

[136] *Marsh*, 721 F.2d at 771.

settling the lawsuit that followed HUD's decision, Alma agreed to obtain a section 404 permit from the Corps before proceeding further.[137]

As part of the process to obtain the permit, the Corps held a public hearing.[138] The court noted that at the hearing opponents to the project "included nearly all federal agencies involved with conservation and environmental issues: the EPA; the Executive Office of the President, Council on Environmental Quality ('CEQ'); FWS; and the Bureau of Outdoor Recreation ('BOR') . . . ."[139] Several non-government environmental groups also opposed the project.[140] Although the District Engineer recommended denying the permit, the Corps continued to investigate it.[141] When the FWS issued a mitigation study, proposing the creation of "green tree reservoirs" to ameliorate the loss of some 1,400 acres of swamp, the Corps eventually agreed to issue the permit, contingent on the mitigation plan being implemented.[142] After several more studies, and another public hearing, EPA, FWS, and BOR withdrew their objections to the permit and thus withdrew their objections to the project.[143]

The National Wildlife Federation (NWF) then filed suit, arguing in part, that the adoption of the mitigation plan required the preparation of an SEIS.[144] Turning to *Environmental Defense Fund v. Marsh*, the Eleventh Circuit noted:

> '[t]he legal standard of the need for a supplemental EIS . . . is whether the post-[original EIS] changes in the [project] will have a 'significant' impact on the environment that has not previously been covered by the [original] EIS.' If a "significant" impact on the environment will result, either "in qualitative or quantitative terms," from subsequent project changes, an SEIS is required.[145]

The project's proponents argued that after the extensive studies both the Corps and EPA agreed the mitigation plan would have no new adverse effect on the environment.[146] However, the court was unhappy with that argument, noting that "[n]either of these agencies nor the Alma officials focused on the degree of mitigation, the beneficial impact, of the Mitigation Plan."[147] The Eleventh Circuit was bound

---

[137] *Id.*

[138] *Id.* at 772.

[139] *Marsh*, 721 F.2d at 772.

[140] *Id.*

[141] *Id.*

[142] *Id.* at 772-73.

[143] *Id.* at 773.

[144] *Marsh*, 721 F.2d at 782.

[145] *Id.* (quoting *Marsh*, 651 F.2d at 991).

[146] *Marsh*, 721 F.2d at 782.

[147] *Marsh*, 721 F.2d at 782.

by both Fifth Circuit precedent and its own from its view in *Environmental Defense Fund v. Marsh,* when the court:

> [M]ade clear that even if post-EIS changes in a project are *beneficial* to the environment or are intended to mitigate environmental impact, if those changes are significant, a supplemental statement is required: "The proper question is not the intent behind the actions, but the significance of the environmental impacts. And even if the Corps was correct in deciding that the new land use will be beneficial in impact, a beneficial impact must nevertheless be discussed in an EIS, so long as it is significant. NEPA is concerned with all significant environmental effects, not merely adverse ones."[148]

Unsurprisingly, the Eleventh Circuit interpreted *Environmental Defense Fund v. Marsh* the same way that the appellants in *Coliseum Square* did, that is, if changes to the EIS result in a new significant beneficial impact, then an SEIS is required. Accordingly, when the Eleventh Circuit concluded that "a number of proposed project changes . . . are likely to have a significant, though beneficial, impact on the environment . . . ," went on to say, that "[g]iven the plan's detailed proposals for mitigating any adverse environmental effects resulting from the creation of Lake Alma, as well as the role of the plan in allaying the environmental concerns of all relevant federal agencies, we conclude that the Mitigation Plan will have a significant qualitative environmental impact."[149] The court also spoke to this conclusion in a footnote that on one hand tends to illuminate their reasoning, and on the other, highlights the problem with it. Footnote 22 reads:

> We emphasize that we have no quarrel with the conclusion that the GTRs will cause no impact on water quality. The Mitigation Plan was intended to mitigate the effect of the project on wildlife considerations. It is this significant impact that warrants an SEIS. If there were no significant impact from the plan it would not qualify as a Mitigation Plan at all. We defer to the judgment of the FWS and the Corps that it is indeed a Mitigation Plan.[150]

It is indisputable the Eleventh Circuit has held here that beneficial significant impacts, which were not discussed in the original EIS, necessitate an SEIS. The way the court reached this conclusion, however, has three major problems. First, the analysis relies on *Environmental Defense Fund v. Marsh*, which was based on the outdated and no longer valid or applicable reasoning from *Hiram Clarke*. Second, even if a court concluded a beneficial significant impact could trigger the need for an SEIS or an EIS, it is problematic to include a mitigation plan in that category.

---

[148] *Id.* at 782-83 (emphasis in original) (quoting *Marsh*, 651 F.2d at 993).

[149] *Marsh*, 721 F.2d at 784.

[150] *Marsh*, 721 F.2d at 784 n. 22.

This will be discussed in greater detail below when examining a mitigated FONSI. However, a mitigation plan, by definition, is not an independent significant effect.[151] It is rather a lessening, or mitigating, of an otherwise pre-existing adverse effect. Mitigation has been regularly accepted and even encouraged by CEQ to minimize impacts such that they fall below the threshold of significance.[152] This mitigation lessens pre-existing adverse impacts that otherwise would have created significant adverse effects and required an EIS.

Third, defining mitigation as an independent significant effect which can trigger the need for an SEIS provides a perverse incentive for agencies to avoid adopting mitigation measures once their EIS has been filed. Given that the U.S. Supreme Court has held an agency does not have to have a fully developed mitigation plan to have a complete EIS, it would be in an agency's best interest to avoid mitigation where possible after the EIS is filed. [153] Otherwise, an agency could find itself in court, and/or having to start the formal EIS process over with an SEIS, simply because they mitigated the adverse effects of their project. This perverse incentive to avoid beneficial effects is one of the problems with any holding which concludes that beneficial impacts trigger the need for an EIS or SEIS, as the results can actually run contrary to the purpose of NEPA. Including mitigation as an independent effect only exacerbates the problem.

Finally, while it is possible to try and distinguish this case as referring *only* to the requirement for an SEIS, the argument cannot be supported. Because the Eleventh Circuit relied on the standard expressed in *Environmental Defense Fund v. Marsh*, it is the same standard for when an EIS is required.[154] The Eleventh Circuit has quoted that exact language in other cases, noting as in the Fifth Circuit, the standard for determining when an SEIS is required is "essentially the same" as the standard for determining when an EIS is required.[155] Since the court held that changes to the project that result in a significant, though beneficial, impact require an SEIS, the same would be true for an EIS. Under *National Wildlife Federation*, if a project has a significant impact, whether beneficial or adverse, an EIS is required.

---

[151] *See infra* Part II.D.2.

[152] Final Guidance for Federal Departments and Agencies on the Appropriate Use of Mitigation and Monitoring and Clarifying the Appropriate Use of Mitigated Findings of No Significant Impact, 76 Fed. Reg. 3843-3853, 3843 (Jan. 21, 2011).

[153] *See* Robertson v. Methow Valley Citizens Council, 490 U.S. 332 (1989) (court held NEPA does not impose duty to include a fully developed mitigation plan in each EIS).

[154] *Marsh*, 721 F.2d at 782.

[155] *Sierra Club*, 295 F.3d at 1215-16 (quoting *Marsh*, 651 F.2d at 993).

4. The Sixth Circuit

In 1995, the Sixth Circuit also addressed the question of the beneficial impact EIS.[156] This was the first time a circuit court looked specifically at the CEQ regulations and the definition of "significantly" since the new regulations were published in 1978. In *Friends of Fiery Gizzard v. Farmers Home Admin.*,[157] the Farmers Home Administration (FmHA) funded the construction of a reservoir on Big Fiery Gizzard Creek to provide drinking water for the town of Tracy, Tennessee.[158] Several sites for a reservoir had been considered and the site selected was approved by EPA, FWS, the Corps, the Tennessee Valley Authority, the state Historical Commission, and the Tennessee Department of Environment and Conservation.[159] FmHA prepared an environmental assessment and issued a finding of no significant impact, concluding that the project would have no adverse impacts.[160] The lawsuit that followed alleged that since the project would have a significant *beneficial* environmental impact, an EIS was required before the project could go forward.[161]

It was clear from the record the project would have a beneficial impact on the residents of Tracy City by providing them with an assured source of clean water.[162] And as the Fifth and Eleventh Circuits concluded, it is possible to construe NEPA as including beneficial impacts as triggering the need for an EIS. However, the Sixth Circuit immediately noted that "[t]he statute . . . must be read in light of the implementing regulations."[163] While NEPA itself does not provide a definition for what "significantly affecting the quality of the human environment"[164] might mean, the CEQ regulations do provide a definition for "significantly."[165] As noted above, those regulations specify that whether an action has a significant effect such that an EIS might be required turns on an individual assessment of its context and intensity.[166] The court reasoned:

> In deciding, on the basis of the assessment, whether the proposed action is one affecting the quality of the environment "significantly," the agency must look at both the "context" of the action and its "intensity." 40 C.F.R. § 1508.27(a) and (b). "Intensity," § 1508.27(b) explains, means "the severity of impact." This choice

[156] *See Friends of Fiery Gizzard*, 61 F.3d at 502-03.

[157] 61 F.3d 501 (6th Cir. 1995).

[158] *Id.* at 503.

[159] *Id.*

[160] *Id.*

[161] *Id.* at 504 (emphasis added).

[162] *Friends of Fiery Gizzard*, 61 F.3d at 504.

[163] *Id*.

[164] 42 U.S.C. 4332(C).

[165] *See* 40 C.F.R. § 1508.27.

[166] *Id.*

> of adjectives is significant, we think; one speaks of the severity of *adverse* impacts, not *beneficial* impacts.[167]

Looking beyond the regulations, the court also addressed the purpose of NEPA: "One of the central purposes of NEPA, after all, is to 'promote efforts which will . . . stimulate the health and welfare of man.' 42 U.S.C. § 4321. Time and resources are not unlimited, as the Supreme Court has reminded us . . . ."[168] With that in mind, the court found that, "the health and welfare of the residents of Tracy City will not be 'stimulated' by the delays and costs associated with the preparation of an environmental impact statement that would not even arguably be required were it not for the project's positive impact on health and welfare."[169]

The direction from CEQ in implementing NEPA was also persuasive to the court: "The regulations of the Council on Environmental Quality direct federal agencies 'to make the NEPA process *more* useful to decision makers and the public,' not less useful; 'to *reduce* paperwork and the accumulation of extraneous background data,' not expand them; and 'to emphasize *real* environmental issues and alternatives' . . . ."[170] Noting that this was the reason the environmental assessment process was created in the first place, the court stated, "[i]t would be anomalous to conclude that an environmental impact statement is necessitated by an assessment which identifies beneficial impacts while forecasting no significant adverse impacts, when the same assessment would not require the preparation of an impact statement if the assessment predicted no significant beneficial effect."[171]

Quite simply, the court recognized that requiring an EIS for a beneficial impact would provide no benefits and would in fact, be contrary to the purpose of NEPA. With this holding, the Sixth Circuit provided an opinion that was based on the current binding implementing regulations, which are entitled to substantial deference.[172] In doing so, it reached the opposite conclusion of the Eleventh Circuit and created the current split in the circuits. However, the Sixth Circuit also reached the correct conclusion.

---

[167] *Friends of Fiery Gizzard*, 61 F.3d at 504 (citing 40 C.F.R. § 1508.27 (emphasis added)).

[168] *Friends of Fiery Gizzard*, 61 F.3d at 505 (citing 42 U.S.C. § 4321 (2012); *Metropolitan Edison Co. v. People Against Nuclear Energy,* 460 U.S. 766, 776 (1983); *Vermont Yankee Nuclear Power Corp. v. Natural Resources Defense Council, Inc.,* 435 U.S. 519, 551 (1978)).

[169] *Friends of Fiery Gizzard*, 61 F.3d at 505.

[170] *Friends of Fiery Gizzard*, 61 F.3d at 505 (emphasis in original) (quoting 40 C.F.R. § 1500.2(b) (1995)). The current regulation referenced by the court can be found at 40 C.F.R. § 1502 (2012).

[171] *Friends of Fiery Gizzard*, 61 F.3d at 505.

[172] *See Andrus*, 442 U.S. at 357.

5. Other Cases

There are two other lines of cases that have been cited as requiring an EIS for projects with beneficial significant impacts. The first deals with claims of exemption from the NEPA process altogether, such as cases dealing with the designation of critical habitat.[173] A claim of exemption from NEPA compliance is not the same as requiring an EIS for beneficial significant impacts. There is no question that in most federal actions, an agency must demonstrate NEPA compliance by completing an EA, an EIS, or documented reliance on a CATEX. There is no categorical exemption from NEPA compliance for beneficial impacts, and the agency must still utilize one of the above approaches. Accordingly, as other literature has demonstrated, cases holding that an activity is not exempt from NEPA compliance cannot be relied upon for the proposition that a significant beneficial impact requires the preparation of an EIS.[174]

The second line of cases arises when a project has significant impacts that are both adverse and beneficial, but overall, will result in a net benefit to the environment.[175] Courts have held that an EIS is still required for these projects and note that an argument that NEPA may be avoided entirely because the overall impact is beneficial is contrary to CEQ regulations.[176] The CEQ regulations make clear that a "significant effect may exist even if the Federal agency believes that on balance the effect will be beneficial."[177] This has also been addressed completely in other literature, making clear that this line of cases deals with actions that *do* have significant adverse impacts, though they may include beneficial effects as well.[178]

B. Statutory Construction

The language in section 102 of NEPA is broad, and can be read to require an EIS for *any* significant impact, including beneficial impacts. The text calling for an EIS requires the agency to:

> (C) include in every recommendation or report on proposals for legislation and other major Federal actions significantly affecting the quality of the human environment, a detailed statement by the responsible official on—

[173] *See, e.g.*, Douglas County v. Babbit, 48 F.3d 1495 (9th Cir. 1995).

[174] *See* Goho, *supra* note 72, at 379-80 (article provides discussion of cases claiming an exemption from NEPA compliance and the insufficiency of this argument for application to beneficial impacts).

[175] *See, e.g.*, Envtl. Prot. Info. Ctr. v. Blackwell, 389 F. Supp. 2d 1174 (N.D. Cal. 2004).

[176] *Envtl. Prot. Info. Ctr.*, F. Supp. 2d. at 1197.

[177] 40 C.F.R. § 1508.27 (2012).

[178] *See* Goho, *supra* note 72, at 380-81 (emphasis added).

> (i) the environmental impact of the proposed action,
>
> (ii) any adverse environmental effects which cannot be avoided should the proposal be implemented . . . .[179]

The real question is what is meant by "significantly affecting" in this section, and does that include beneficial impacts? In looking at the two requirements cited, and attempting to give each one an independent meaning, it would be plausible to conclude that Congress intended beneficial impacts to be included in the subsection (i) requirement to address the environmental impact, since subsection (ii) specifically addresses adverse effects. Yet, as the Supreme Court has indicated, "[w]e do not, however, construe statutory phrases in isolation; we read statutes as a whole."[180] Furthermore, when " . . . interpreting a statute, the court will not look merely to a particular clause in which general words may be used, but will take in connection with it the whole statute . . . and the objects and policy of the law . . . ."[181]

To that end, it is important to look at the purpose of the statute. In 2009, President Barack Obama indicated that "NEPA was enacted to promote efforts that will prevent or eliminate damage to the environment . . . ."[182] Then in 2011, the chair of CEQ also stated that NEPA was enacted to "prevent or eliminate damage to the environment."[183] Both statements quote from the congressionally declared purpose of NEPA:

> To declare a national policy which will encourage productive and enjoyable harmony between man and his environment; to promote efforts which will prevent or eliminate damage to the environment and biosphere and stimulate the health and welfare of man; to enrich the understanding of the ecological systems and natural resources important to the Nation; and to establish a Council on Environmental Quality.[184]

As the Sixth Circuit concluded, this purpose would be frustrated by an interpretation that would require an agency to expend substantial time and money to prepare an EIS before going forward with a project that was already in keeping with the declared intent to eliminate damage to the environment and stimulate the health and

---

[179] 42 U.S.C. § 4332(C)(i)-(ii).

[180] United States v. Morton, 467 U.S. 822, 828 (1984) (citing, *Stafford*, 444 U.S. at 535).

[181] *Stafford*, 444 U.S. at 535 (quoting Brown v. Duchesne, 60 U.S. 183, 194 (1856)).

[182] Proclamation No. 8469, 75 Fed. Reg. 885-886 (Jan. 7, 2010).

[183] Council on Envtl. Quality, Memorandum from Nancy H. Sutley, Chair, Council on Envtl. Quality, to Heads of Federal Departments and Agencies Appropriate Use of Mitigation and Monitoring and Clarifying the Appropriate Use of Mitigated Findings of No Significant Impact, 2 (Jan. 14, 2011), *available at* http://ceq.hss.doe.gov/current_developments/docs/Mitigation_and_Monitoring_Guidance_14Jan2011.pdf [hereinafter Sutley Memorandum].

[184] 42 U.S.C. § 4321 (2013).

welfare of man.[185] Such a requirement would frustrate NEPA's declared purpose, as it would create an incentive for agencies to avoid actions that would "eliminate damage to the environment."[186] Worse yet, it could actually prevent many beneficial actions, as it would make them too expensive or too time-consuming to implement.

The REPI project cited in the beginning of this article illustrates how reading NEPA to require an EIS for beneficial impacts is actually contrary to NEPA, when read as a whole. As pointed out above, REPI funds are not unlimited and the goal of the agency to create a buffer could be met by purchasing land and leaving it untouched.[187] There is no need to engage in projects that actually enhance the environment. However, by doing so, the agency not only meets the declared purpose of NEPA by "[encouraging] productive harmony between man and his environment. . ." and "[eliminating] damage to the environment . . . ,"[188] but also meets the objectives of the declared national policy to "attain the widest range of beneficial uses of the environment without degradation . . ." and to "preserve important . . . natural aspects of our national heritage and maintain, wherever possible, an environment which supports diversity . . . ."[189] Finally, the project is also perfectly in accord with the declared national policy "to use all practicable means and measures, including financial and technical assistance, in a manner calculated to foster and promote the general welfare, to create and maintain conditions under which man and nature can exist in productive harmony . . . ."[190]

If an EIS were required for this project, however, it is unlikely that sufficient funds would be available to undertake it. Certainly, fewer projects of this type could be executed. Most likely, the agency would simply avoid the actions that enhance the environment so as to avoid any significant, though beneficial, effects. It is hard to conclude that eliminating projects that actually meet the goals of NEPA, limiting their number, or even precluding their beneficial environmental impacts could be read to be in keeping with the policies or purpose of the Act.

Accordingly, another possible interpretation of section 102 (C) is that subsection (i) simply requires a statement of the overall environmental impacts, including effects that could be avoided with appropriate mitigation or by choosing environmentally friendly alternatives. Subsection (ii) then requires special attention paid to any unavoidable adverse effects. This has the effect of necessitating a discussion of mitigation in identifying the avoidable and unavoidable adverse effects. It does not necessarily follow that this section requires beneficial significant impacts

---

[185] *Friends of Fiery Gizzard*, 61 F.3d at 505.

[186] 42 U.S.C. § 4321 (2013).

[187] *See supra* note 22, at 9. (common uses of REPI)

[188] 42 U.S.C. § 4321.

[189] *Id.* § 4331(b).

[190] *Id.* § 4331(a).

to trigger the need for an EIS. This interpretation of NEPA appears to be the one embraced by CEQ, with the creation of the distinction between the EA and the EIS.

Recognizing that NEPA is also enacted to provide information to the public, the EA, created by CEQ regulations, can provide the public with the overall statement of the environmental impact of a proposed action required by Section 102 (C) (i), when there are no significant adverse impacts.[191] It also demonstrates NEPA compliance, documenting the lack of impacts significantly affecting the quality of the human environment. The more detailed EIS would provide special attention and greater detail for any unavoidable significant adverse impacts, as required by section 102 (C) (ii).[192] When there are no unavoidable significant adverse impacts, it makes sense that the document would be shorter and an EA would be appropriate. CEQ has stressed the importance of reducing paperwork and focusing on real environmental issues.[193] This interpretation is further supported by the acceptance of a mitigated FONSI, where otherwise significant impacts are mitigated to something less than significant and an EA has been found to be appropriate.[194] It is compelling that CEQ has allowed a line to be drawn between an EA and the need for an EIS by the avoidance, or mitigation, of adverse impacts.[195] This fits neatly into the interpretation that *only* when there are unavoidable significant adverse impacts is the more detailed EIS required.

The problem with this argument is that NEPA only requires an environmental statement if there *are* significant environmental impacts. So the counterargument is, why would you need a statement at all, EA or otherwise, if beneficial impacts are not included in significant environmental effects, and the project only resulted in significant beneficial impacts? The answer, and the reason that such a counterargument fails, is found in the way that CEQ has interpreted NEPA. Under CEQ regulations, nearly all federal actions require some demonstration of NEPA compliance. An action must fit a CATEX or the agency must prepare either an EA or EIS.[196] This is true even for actions that an agency knows will not have a significant environmental impact or even no environmental impact at all. The purposes of NEPA are thus served, in providing information to the public, and demonstrating that environmental effects have been considered and the action will not have significant unavoidable adverse impacts.

---

[191] 42 U.S.C. § 4332(C).

[192] 42 U.S.C. § 4332(C).

[193] 40 C.F.R. § 1502 (2012).

[194] *See* Final Guidance for Federal Departments and Agencies on the Appropriate Use of Mitigation and Monitoring and Clarifying the Appropriate Use of Mitigated Findings of No Significant Impact, 76 Fed. Reg. at 3843.

[195] *Id.*

[196] 40 C.F.R. § 1502.

In the end, finding the line of significance between an EA and an EIS is a regulatory distinction and not one based on statutory interpretation, save that it may illuminate the approach CEQ has taken to implement the statute. While the regulations do support the interpretation that by simply including subsections (i) and (ii) in 102(C), Congress did not automatically intend for beneficial impacts to equate to what is meant by "significantly affecting the quality of the human environment . . . ,"[197] they do not provide a definitive answer. In the end, exactly what is meant by "significantly affecting" in section 102 is unclear.[198] In such a case, "[i]n order to 'give [the Act] such a construction as will carry into execution the will of the Legislature . . . according to its true intent and meaning' . . . we turn to the legislative history."[199]

C. Legislative History

The House and the Senate both presented bills to establish a national environmental policy and an executive council for environmental quality.[200] The proposed policy contained strong language, directing the use of all "practical means and measures," to comply with its directives.[201] However, there was still a fear that a policy alone would not be enough.[202] Senator Henry "Scoop" Jackson, the chairman of the Senate Interior and Insular Affairs Committee, related his fears:

> I have been concerned with the inadequacy of the policy declaration in the bill I have introduced. Obviously, this is not enough . . . [W]hat is needed in restructuring the governmental side of the problem is to legislatively create those situations that will bring about an action forcing procedure the departments must comply with. Otherwise, these lofty declarations are nothing more than that.[203]

Accordingly, the committee's view was that to ensure agencies embraced the new environmental policy, any legislation needed to include action-forcing procedures.[204] With that in mind, the committee report explained:

> To remedy present shortcomings in the legislative foundations of existing programs, and to establish action-forcing procedures which will help to ensure that the policies enunciated in section

[197] 42 U.S.C. § 4332(C).

[198] *Id.*

[199] *Stafford*, 444 U.S. at 535 (quoting Brown, 60 U.S. at 194 (citation omitted).

[200] Luther, *supra* note 27, at 2-3.

[201] S. Rep. No. 91-296, at 1-2.

[202] *See* Ferlo et al., *supra* note 3, at 2.

[203] Luther, *supra* note 27, at 1 (quoting *Hearing on S.1075 and S. 1752 Before the S. Comm. on Interior and Insular Affairs,* 91st Cong. 116 (1969) (statement of Sen. Henry Jackson, Chairman, S. Committee on Interior and Insular Affairs)).

[204] S. Rep. No. 91-296, at 19.

> 101 are implemented, section 102 authorizes and directs that the existing body of Federal law, regulation, and policy be interpreted and administered to the fullest extent possible in accordance with the policies set forth in this Act.[205]

The Senate committee report does not specifically address what is meant by "significantly affecting the quality of the human environment," however, it is the only congressional report that speaks to the action forcing provisions in Section 102 and provides the best insight into the intent of this provision.[206]

The text of section 102 in the Senate version of NEPA, S. 1075, was slightly different than what ultimately made its way to the President and these differences explain what is actually meant in subsections (i) and (ii).[207] Table 1 highlights those differences.

Table 1

| Section 102 (C) S. 1075 | Section 102 (C) of the final NEPA |
|---|---|
| (C) include in every recommendation or report on proposals for legislation and other major Federal actions significantly affecting the quality of the human environment, a finding by the responsible official that — | (C) include in every recommendation or report on proposals for legislation and other major Federal actions significantly affecting the quality of the human environment, a detailed statement by the responsible official on — |
| (i) the environmental impact of the proposed action has been studied and considered; | (i) the environmental impact of the proposed action, |
| (ii) any adverse environmental effects which cannot be avoided by following reasonable alternatives are justified by other stated considerations of national policy; | (ii) any adverse environmental effects which cannot be avoided should the proposal be implemented, |
| (iii) local short-term uses of man's environment are consistent with maintaining and enhancing long-term productivity; and that | (iii) alternatives to the proposed action, |
| (iv) any irreversible and irretrievable commitment of resources are warranted.[205] | (iv) the relationship between local short-term uses of man's environment and the maintenance and enhancement of long-term productivity, and |
| | (v) any irreversible and irretrievable commitments of resources which would be involved in the proposed action should it be implemented.[206] |

[205] *Id.* at 19-20.

[206] Ferlo et al., *supra* note 3, at 2.

[207] S. Rep. No. 91-296, at 2.

Despite the differences, if the general intent of the provision remains the same in what was ultimately passed, as it was in the Senate bill, an argument that beneficial effects were meant to be included in the requirement for an EIS makes little sense. The original language calls for a certification, and requires a study of the overall environmental impact, with special attention paid to, and justification for, unavoidable adverse consequences. In the version that was ultimately signed into law, the requirement to discuss alternatives was given additional emphasis. This is weaker than a required certification and justification for unavoidable consequences, but still requires federal agencies to consider how to avoid adverse effects. Some alternatives will obviously have an adverse environmental impact that *can* be avoided. These would still be discussed under subsection (i). Subsection (ii), however, calls for special attention for any adverse impacts that cannot be avoided under *any* alternative and tracks with subsection (ii) of the original language. The intent of both the draft and final provision is to ensure that the government takes steps to avoid adverse consequences whenever possible.

The main differences between subsections (i) and (ii) in the Senate bill and the law that was ultimately passed appears to be the separation of the requirement to address alternatives to the action, and the deletion of a requirement for an actual finding that adverse effects are justified in light of other policy concerns. These are significant differences, as had S. 1075 passed in its original form, NEPA may not have been only a procedural statute, but could have actually called for specific environmental results. However, the original wording is still very suggestive of the intent of the final provisions.

The section-by-section analysis in the report provides further illumination. Subsection C was intended to require actual findings by the responsible official with regard to major federal actions significantly affecting the quality of the human environment.[210] The finding in subsection (i) was intended to be "that the environmental impact of the proposed action has been studied and that the results of the studies have been given consideration in the decisions leading to the proposal."[211] This generally just expresses the need to consider environmental impacts in agency decision making. The finding in subsection (ii) was intended to be more dramatic, being that:

> Wherever adverse environmental effects are found to be involved, a finding must be made that those effects cannot be avoided by following reasonable alternatives which will achieve the intended purposes of the proposal. Furthermore, a finding must be made that the action leading to the adverse environmental effects is justified

[208] *Id.*

[209] 42 U.S.C. § 4332(C).

[210] S. Rep. No 91-296, at 20.

[211] *Id.*

by other considerations of national policy and those other considerations must be stated in the finding.[212]

As noted above, had the provision been enacted as originally written in S. 1075, it would have created a statute that directed substantive results or a finding that environmental quality was outweighed by other considerations. The changes seem to indicate that Congress was not comfortable with forcing that level of substantive requirement on federal agencies. In taking out the provision, there may have been a compromise. The proposed language required a finding that the adverse effects could not be avoided by reasonable alternatives and that the effects were justified. The enacted legislation instead broke the process down, calling for the discussion of environmental impacts for all alternatives, and highlighting the adverse impacts that could not be avoided under any alternative. This does two things. It highlights the need for alternatives that avoid adverse impacts where possible and necessitates a discussion of mitigation.

Looking at the original draft of 102 (C), the inclusion of a section requiring a discussion of over-all impacts and a discussion of why adverse impacts cannot avoided is harmonious and makes perfect sense. The two provisions have nothing to do with requiring the discussion of beneficial impacts and each has its own distinct purpose. While the redrafted version is less clear, the original intent of the provisions remains the same—to address the overall environmental impacts for all alternatives, with special attention paid to unavoidable adverse impacts under any alternative. By highlighting the need to discuss reasonable alternatives, Congress has ensured that while there may not be a substantive mandate, at least the agency will know which alternative presents the best environmental outcome. The general purpose of the bills, as expressed in the legislative history, supports this interpretation. There is nothing to suggest that in changing the provisions, Congress intended beneficial impacts to be included in "significantly affecting."

The discussion of the purposes of both the Senate and House bills both focus on halting environmental degradation and solving current and future environmental problems. The House bill, H.R. 12549, called for the formation of an executive council and would have added an environmental policy to existing statutes.[213] In the very first paragraph of the report, Congress declared that the purpose of the bill was "to create a council that can advise the President, Congress and the American people . . . on steps which may and should be taken to improve the quality of the environment."[214] The House Committee felt that "[a]n independent review of the interrelated problems associated with environmental quality is of critical impor-

[212] *Id.*

[213] *See* H.R. Rep. No. 91-378 (1969).

[214] *Id.* at 115.

tance if we are to reverse what seems to be a clear and intensifying trend toward environmental degradation."[215]

The House bill, in addition to the creation of the council, called for a policy section that would, "recognize the impact of man's activities upon his environment and the critical importance of making that impact less adverse to his welfare."[216] Thus, while the House version of the bill was limited to the creation of CEQ and a declaration of policy, it still attempted to find ways to halt environmental degradation and solve the pressing environmental problems of the day, as illustrated by the committee's use of a quote from the New York Times:

> By land, sea, and air, the enemies of man's survival relentlessly press their attack. The most dangerous of all these enemies is man's own undirected technology. The radioactive poisons from nuclear tests, the runoff into rivers of nitrogen fertilizers, the smog from automobiles, the pesticides in the food chains, and the destruction of topsoil by strip mining are examples of the failure to foresee and control the untoward consequences of modern technology.[217]

The Senate bill was also clearly focused on halting environmental degradation. The committee began: "It is the unanimous view of the members of the Interior and Insular Affairs Committee that our Nation's present state of knowledge, our established public policies, and our existing governmental institutions are not adequate to deal with the growing environmental problems and crises the nation faces."[218] The report then catalogues a long list of environmental problems demonstrating the environmental failures of the nation, including "the loss of valuable open space; inconsistent and, often, incoherent rural and urban land-use policies; critical air and water pollution problems; diminishing recreational opportunity; continuing soil erosion; needless deforestation; the decline and extinction of fish and wildlife species; . . . and many, many other environmental quality problems."[219] Thus, the committee declared that "[t]he purpose of S. 1075 is, therefore, to establish a national policy designed to cope with environmental crisis, whether present or impending."[220]

To address this challenge, the committee indicated NEPA would contribute to better federal response to environmental decision-making in five ways.[221] These five benefits are: clarifying that agencies *do* have authority to consider environmental factors in making decisions; the inclusion of broad national environmental

---

[215] H.R. Rep. No. 91-378, at 117.

[216] *Id.* at 123.

[217] H.R. Rep. No. 91-378, at 117 (quoting a *New York Times* editorial).

[218] S. Rep No. 91-296, at 4.

[219] *Id.*

[220] *Id.* at 9.

[221] *Id.*

goals and an action-forcing provision; authority to conduct environmental studies and surveys; the establishment of CEQ; and the requirement that CEQ provide an annual environmental report.[222] Only two statements however, directly bear on this discussion. The committee indicated that the action-forcing provision, the requirement to produce an EIS, was "designed to assure that all Federal agencies plan and work toward meeting the challenge of a better environment."[223] The very next sentence, while addressing a separate factor, is even more illuminating: "One of the major factors contributing to environmental abuse and deterioration is that actions—often actions having irreversible consequences—are undertaken without adequate consideration of, or knowledge about, their impact on the environment."[224]

These two sentences describe one of the two recognized purposes for producing an EIS—to provide agencies with enough information to adequately consider environmental affects in making decisions. It is telling that these sections both indicate that the action forcing provision, or EIS, is geared to forcing agencies to "work toward a better environment . . . " and halting "environmental abuse and deterioration . . ."[225] There is nothing in these "five major ways" in which NEPA will improve agency decision-making that indicates the action forcing provision of NEPA was meant to apply to actions that had no adverse impact on the environment.[226] Quite the contrary, the committee report indicates that NEPA was intended to help the government plan and work toward a better environment, and force agencies to consider environmental impacts before taking actions that would have unavoidable adverse effects. The focus in both committee reports remains on avoiding or minimizing environmental degradation. Any interpretation of NEPA that would frustrate that goal is contrary to the collective committees' declared purpose of the act.

An argument can be made that an EIS for beneficial impacts is necessary to satisfy the other recognized purpose of producing an EIS—to adequately inform and involve the public in agency decision-making. The Senate Committee report indicated that "[a] primary purpose of the bill is to restore public confidence in the Federal Government's capacity to achieve important public purposes and objectives and at the same time to maintain and enhance the quality of the environment."[227] Yet even with this declared purpose by the Senate, the requirement for public participation in the NEPA process is almost non-existent in the language of the statute itself. The current requirement for public participation is based instead almost entirely in regulation. It is possible that this statement in the report, quoted above, did not indicate a desire to involve the public to the extent the regulations ultimately did. Yet

[222] *Id.* at 9-10.

[223] *Id.* at 9.

[224] S. Rep No. 91-296, at 9.

[225] *Id.*

[226] *Id.*

[227] *Id.* at 8.

public participation is consistent with the legislative history and has been recognized by the courts as one of the two purposes of NEPA.[228]

While limited support for requiring public participation can be found in NEPA's policy statement, "it is the continuing policy of the Federal Government, in cooperation with State and local governments, and other concerned public and private organizations . . . ,"[229] Section 102 requires agencies, "make available to States, counties, municipalities, institutions, and individuals, advice and information useful in restoring, maintaining, and enhancing the quality of the environment."[230] However, the explicit requirement for public participation is found in CEQ's implementing regulations.[231] While the legislative history indicates a desire to involve the public in environmental agency decision making, any argument that an EIS for beneficial impacts is necessary to meet this purpose, must still inevitably turn on the regulations promulgated by CEQ.

These regulations provide an elegant solution, ensuring that this second primary purpose of NEPA is met even when there are no significant effects on the quality of the environment. In most cases, the agency must still prepare an EA that will be available to interested parties and the public.[232] While the requirement for public participation in the drafting of an EA is not as extensive as that required for an EIS, it is still sufficient, given the lower risk to the environment of a project that has no significant environmental impacts. The EA thus satisfies NEPA's purpose of involving and informing the public, without the expense and delay of an EIS. To fully explore this argument, it is necessary to turn to the source of the specific requirement, the regulations promulgated by CEQ.

D. CEQ Regulations

In 1978, CEQ promulgated regulations for implementing the procedural aspects of NEPA.[233] These regulations have remained almost entirely unchanged for nearly 35 years. The 1971 regulations operated as mere guidance for federal agencies, which as noted above, did not result in a uniform approach to the statute.[234] The 1978 regulations, however, were binding on all federal agencies and have been held to be entitled to substantial deference by the courts.[235]

---

[228] *See Baltimore Gas & Elec. Co.*, 462 U.S. at 97.

[229] 42 U.S.C. § 4331.

[230] *Id.* § 4332(G).

[231] *See* 40 C.F.R § 1503.

[232] *See* 40 C.F.R. § 1501.

[233] Implementation of Procedural Provisions of NEPA, 43 Fed. Reg. 55,978-55,990 (Nov. 29, 1978).

[234] *See* Statements on Proposed Federal Actions Affecting the Environment, 36 Fed. Reg. 7724-7729 (Apr. 23, 1971).

[235] *See Andrus*, 442 U.S. at 357.

1. Defining Significant Effects on the Environment

While the regulations do not provide a bright-line rule as to what might be considered a significant impact on the environment, the definitions were substantially expanded and include a fairly detailed definition of "significantly," as well as a helpful definition of effects.[236] In first reading the statute, it might seem that there would be some disagreement as to what qualifies as a major action for purposes of significantly affecting the environment. However, CEQ has stated that, "Major," as defined by the regulations as part of a major federal action, "reinforces but does not have a meaning independent of significantly."[237] Therefore, in determining what actions require an EIS, the key is not whether the action is a major one, but whether the action would have a significant effect on the quality of the human environment.

As noted in the discussion of *Friends of Fiery Gizzard v. Farmers Home Admin.*, the term "significantly" is not given a simple definition in the regulations.[238] Instead, guidelines are provided to help determine when an action has significant effects. Determining if an effect might be significant requires "consideration of both context and intensity."[239] Context means that the "significance of the action must be analyzed in several contexts such as society as a whole (human, national), the affected region, the affected interests, and the locality. Significance can vary with the setting of the proposed action."[240] In other words, if all the environmental effects are limited to one small geographic area, such as the construction of a parking lot, significance must be analyzed in the context of that local geographic area. Conversely, if the effects are felt across the nation as a whole, such as the proposed adoption of a new governmental program or standard, significance must be analyzed in the context of how it will affect the entire nation.

Intensity, as it is defined in the regulation, "refers to the severity of the impact."[241] In order to determine the intensity of an effect, the regulation provides a list of ten factors for an agency to consider.[242] Most of these factors are straightforward: the degree of risk to the environment; the "degree to which the action affects public health or safety;" the proximity of the action to unique, protected or culturally significant geographic areas; and the degree to which the action might affect a threatened or endangered species.[243] All of these represent adverse effects

---

[236] 40 C.F.R. § 1508 (2012).

[237] 40 C.F.R. § 1508.18.

[238] *See Friends of Fiery Gizzard*, 61 F.3d at 504 (citing 40 C.F.R. § 1508.27).

[239] 40 C.F.R. § 1508.27.

[240] *Id.*

[241] 40 C.F.R. § 1508.27. This language was particularly persuasive to the Sixth Circuit, as it concluded that "one speaks of the severity of *adverse* impacts, not *beneficial* impacts." *Friends of Fiery Gizzard*, 61 F.3d at 504 (emphasis in original).

[242] 40 C.F.R. § 1508.27.

[243] *Id.*

where analyzing the severity of the impact makes sense. However, two of the factors are different. One requires the agency to consider whether the action is connected to other actions which cumulatively might have a significant impact.[244] This prevents agencies from avoiding thorough environmental analysis by breaking projects into multiple parts that individually do not have a significant impact on the environment. The remaining factor is the one that presents the confusion. This factor states that when evaluating intensity, agencies must consider "Impacts that may be both beneficial and adverse. A significant effect may exist even if the Federal agency believes that on balance the effect will be beneficial."[245]

A plausible interpretation of this is that beneficial impacts could be significant. Read in isolation, that is reasonable. But, there is one other definition that also mentions beneficial effects—the definition of "effects." It is important to note that in the regulations, the term "effects" and the term "impacts" are synonymous and used interchangeably. [246] The very last sentence in the definition of effects provides: "Effects may also include those resulting from actions which may have both beneficial and detrimental effects, even if on balance the agency believes that the effect will be beneficial."[247] This section when read literally, implies that in order to have *anything* that would qualify as a beneficial *effect* under NEPA, it must first be part of an action that has *both* beneficial and detrimental effects. If that is the case, then without an adverse impact, we never reach the stage of analyzing the effect's intensity or significance. It is telling that nowhere in the regulations does the term "beneficial effects" ever appear independent of some adverse effect in the same action. This interpretation is also supported by CEQ guidance documents.

In a guide for aligning NEPA with Environmental Management Systems (EMS), CEQ described the NEPA process in part as " . . . forecasting the impacts of a proposed action and reasonable alternatives, and identifying mitigation measures for those impacts prior to making decisions and taking action ('predict-mitigate-implement" model.')"[248] This explanation of NEPA presupposes any analysis of impacts must include adverse impacts. It is significant that in no NEPA regulation, CEQ guidance, CEQ memorandum, or policy document does CEQ ever indicate that beneficial effects must be analyzed for significance, independent of adverse effects. Nowhere are beneficial effects even discussed, absent some adverse effect in the same action.

The most convincing support for the proposition that effects only include those actions with adverse impacts can be found in the CEQ guidelines that predate

---

[244] *Id.*

[245] *Id.*

[246] 40 C.F.R. § 1508.8.

[247] *Id.*

[248] CEQ, Aligning National Environmental Policy Act Process with Environmental Management Systems, A Guide for NEPA and EMS Practitioners 2 (2007).

the current regulations. The definitions of "effect" and "intensity" in the discussion of both beneficial and adverse impacts in the 1978 regulations have very similar language. Both appear to be drawn from language that existed in the 1973 CEQ guidance.[249] Just like the 1978 consideration of intensity, the 1973 guidance also provided a long list of things to consider in evaluating the significance of an impact on the environment.[250] One of those things to consider in determining the significance of an effect was that "Significant effects can also include actions which may have both beneficial and detrimental effects, even if on balance the agency believes that the effect will be beneficial."[251]

This wording is slightly different than the 1978 regulations, but the intent appears to be the same. In this version it is clearer that to have a significant effect, there must be *both* adverse and beneficial effects. To further emphasize this point, toward the latter end of section 1500.6, CEQ explains what is required for an action to significantly affect the environment: "Finally, the action must be one that significantly affects the quality of the human environment either by directly affecting human beings or by indirectly affecting human beings through adverse effects on the environment."[252] Here, CEQ has explicitly stated that for an impact to be significant, it must be an adverse effect.

This language does not exist in the 1978 regulations, but the reason it was removed was not because CEQ intended for beneficial effects to result in the kind of significant impact that would trigger an EIS. Rather, the focus of the impact on the environment that was to be analyzed changed somewhat. As one can see in additions to the factors in evaluating intensity in the 1978 regulations, it is not just the effect on human beings that must be considered. Agencies now must also consider effects to endangered species and unique or scenic geographic areas.[253] Yet even with this change of focus, it would, of course, still have been possible for CEQ to leave in language that expressly stated that impacts must be adverse to be significant.

So why then, was the language from 1973 regulations that expressly indicated an impact must be adverse to rise to the level of significantly affecting the environment, absent from the 1978 regulations? It is impossible to say for sure, but again, this simply is not an issue that arises frequently, and was probably not a priority in the minds of the council when working on the regulations. After all, the procedural provisions that these regulations address were created to force the government take a better environmental approach with less environmental damage. Most of the statements from CEQ discussing the regulations presuppose an adverse environmental impact. Neither CEQ nor the drafters of the legislation likely put

[249] *See* Preparation of Environmental Impact Statements: Guidelines, 38 Fed. Reg. at 20, 551-52.

[250] *Id.*

[251] *Id.*

[252] *Id.*

[253] 40 C.F.R. § 1508.27.

much thought into how to account for government actions that *benefit* the environment, other than to encourage them. Still, the intent that only actions with adverse effects rise to the level of significance remains demonstrated in the purposes of the act, the purpose of the regulations, and the way that CEQ has interpreted the act and regulations in the last 35 years.

2. Purpose of the Regulations and CEQ's Interpretation

The preamble to the regulations in 1978 set out the following purpose; "We expect the new regulations to accomplish three principle aims: To reduce paperwork, to reduce delays, and at the same time to produce better decisions which further the national policy to protect and enhance the quality of the human environment."[254] No good argument can be advanced that requiring an EIS for beneficial impacts reduces paperwork or delays. Both of these purposes in fact, suggest that no EIS should be required when there are no adverse impacts.

CEQ stated that to reduce paperwork, "[t]he environmental analysis is to concentrate on alternatives, which are the heart of the process . . . ."[255] As discussed above in the legislative history, the separate requirement for a discussion of alternatives was intended to focus attention on ways to avoid adverse effects and ensure agencies were aware which alternative produced the least adverse impacts. In keeping with that, CEQ stated the "record of decision must indicate which alternative (or alternatives) considered in the EIS is preferable on environmental grounds."[256] This requirement neatly captures the intent of the alternatives discussion in the legislative history—that of finding the alternative that avoids the greatest adverse environmental impacts. Preparing an EIS when there are no adverse impacts to try to avoid makes little sense and in no way reduces paperwork. As mentioned above, this purpose can best accomplished by an EA.

CEQ indicated that to reduce delays, "If an action has not been categorically excluded . . . but nevertheless will not significantly affect the human environment, the agency will issue a finding of no significant impact as a basis for not preparing an EIS."[257] The regulations provide that the discussion of impacts in an EIS should be limited to what is necessary: "As in a finding of no significant impact, there should be only enough discussion to show why more study is not warranted."[258] If no alternatives produce a significant adverse impact on the environment, it is very hard to justify the additional study that an EIS would provide.

---

[254] Implementation of the Procedural Provisions of NEPA, 43 Fed. Reg. 55,978-55,990, 55,978 (Nov. 29, 1978).

[255] *Id.* at 55,978.

[256] *Id.* at 55,980.

[257] Implementation of the Procedural Provisions of NEPA, 43 Fed. Reg. at 55,979.

[258] 40 C.F.R. § 1502.2.

An argument can be raised that an EIS is needed to accomplish the third purpose, that of making better decisions, but the argument is not well supported. If alternatives are the heart of the EIS process, as quoted above, then the argument would be that an EIS is needed to provide alternatives that will allow the decision-maker to identify the course of action *most* beneficial to the environment. Yet this argument fails, as an EA accomplishes the same thing, in a shorter format. The EA still must discuss alternatives and their impacts on the environment.[259] If one alternative is more beneficial than another, that will still be revealed and can still be relied upon in making decisions. Indeed, viewed in light of the purposes of both the statute and the regulations, once it is demonstrated that there are no adverse impacts, no more study is warranted. This appears to be CEQ's interpretation as well, as demonstrated by the concept of a mitigated FONSI.

CEQ has discussed the mitigated FONSI several times. The basic concept is that a FONSI can be issued even if an action would have a significant impact on the environment if that impact is mitigated as part of the proposal so that the ultimate impact is less than significant.[260] Later guidance from CEQ is suggestive of not just what is expected of mitigated FONSIs, but also when an EA is appropriate in general. As noted above, in discussing the appropriate use of mitigation and mitigated FONSIs the Chair of CEQ noted that "NEPA was enacted to promote efforts that will prevent or eliminate damage to the environment."[261] The mitigated FONSI does that by encouraging agencies to "[commit] to mitigate significant environmental impacts, so that a more detailed EIS is not required."[262]

CEQ and the California Governor's Office recently released a handbook for integrating state and federal environmental review, which explained the NEPA process for a mitigated FONSI: "If the potentially significant impacts can be mitigated to a point where clearly no significant effects would occur, then the lead agency may prepare a Finding of No Significant Impact . . . ."[263] This language presupposes that any significant effect is by nature, adverse. The California Environmental Quality Act (CEQA) process was also explained: "If the project will not have any adverse impacts, or such impacts can be mitigated to a point where clearly no significant effects would occur, the lead agency may adopt a Negative Declaration . . . ."[264]

---

[259] 40 C.F.R. §1508.9.

[260] *See* Forty Most Asked Questions Regarding CEQ's National Environmental Policy Act Regulations, 46 Fed. Reg. 18,026-18,038, 18,038 (Mar. 23, 1981).

[261] Sutley Memorandum, *supra* note 180, at 2.

[262] Final Guidance for Federal Departments and Agencies on the Appropriate Use of Mitigation and Monitoring and Clarifying the Appropriate Use of Mitigated Findings of No Significant Impact, 76 Fed. Reg. at 3843.

[263] CEQ and the California Governor's Office of Planning, NEPA and CEQA: Integrating State and Federal Environmental Reviews, 12 (*Draft for Public Review and Comment*) (March 2013) [hereinafter California Governor's Office NEPA Report].

[264] California Governor's Office NEPA Report, *supra* note 260, at 13. A Negative Declaration is roughly the California equivalent of a FONSI.

This language specifically spells out that a significant effect must be adverse, and it is telling that CEQ and the Governor's office then conclude, "NEPA and CEQA largely dictate the same process for determining the need for an EIS or EIR."[265]

In fact, when highlighting the differences between the two processes, the handbook noted that:

> There is some divergence between the laws in the standard for determining significance. Under CEQA, an EIR is required if substantial evidence supports a *fair argument* that a project *may* have a significant impact, even if other substantial evidence indicates that the impact will not be significant. Under NEPA, more deference is given to the agency's determination based on its assessment of the context and intensity of the potential impacts (40 CFR § 1508.27), where that determination is demonstrated in the NEPA document and supported by the administrative record.[266]

While this is only draft guidance and even in its final version would not amount to a legally binding document, it is nevertheless compelling in its demonstration of how CEQ interprets significant effects. According to this handbook, the real difference between NEPA and a law that specifically requires that effects be adverse to be significant, is that federal agencies receive *more* deference in their determinations of whether an impact is significant.

The NEPA FONSI process presupposes that a significant effect is adverse, the state process requires an effect be adverse to be significant, and the handbook indicates the two processes are largely the same. The conclusion to draw from the language here and in other discussions of the mitigated FONSI, is if you can structure an action such that there are no significant adverse impacts, then a FONSI is appropriate. There can of course be beneficial effects, and these may need to be discussed in NEPA documents such as an EA. But, a significant effect on the environment requiring an EIS only exists where there are significant adverse impacts, and only where it is not possible to mitigate those adverse effects sufficiently.

Critics of this analysis might point out mitigation would not apply to beneficial effects; thus, there can be no mitigated FONSI for beneficial significant impacts and any discussion of a mitigated FONSI would *have* to be based on adverse impacts. This observation, however, would be untrue. It is, of course, possible for agencies to avoid beneficial effects in many cases, such as REPI, where the agency need only obtain land or an easement, as opposed to any action that might actively enhance the environment. In fact, it seems quite likely that should NEPA be interpreted to

---

[265] California Governor's Office NEPA Report, *supra* note 260, at 13. An Environmental Impact Report (EIR) is roughly the California equivalent of an EIS.

[266] California Governor's Office NEPA Report, *supra* note 260, at 13 (emphasis in original).

require an EIS for beneficial significant impacts, agencies would do their best to avoid or "mitigate" beneficial significant impacts. Projects like the one to restore the longleaf pine forest in Georgia, noted at the beginning of this article, would likely not exist. Such a result would be exactly the opposite of what this action-forcing provision of NEPA was intended to produce. Certainly the purpose of helping and encouraging agencies to make better, more environmentally conscious decisions would not be served. Accordingly, such an interpretation cannot be found to be in harmony with the policies and purposes of the act or their implementing regulations. When discussing the procedural provisions of the new regulations CEQ stated:

> Most of the features described above will help to improve decision-making. This, of course, is the fundamental purpose of the NEPA process, the end to which the EIS is a means. Section 101 of NEPA sets forth the substantive requirements of the Act, the policy to be implemented by the "action-forcing" procedures of section 102. These procedures must be tied to their intended purpose, otherwise they are indeed useless paperwork and wasted time.[267]

This is a strong statement on the need for the NEPA document to advance the purposes of the act. Since requiring an EIS for beneficial impacts will not advance the purpose of preventing or eliminating environmental damage, the only remaining purpose of NEPA that could be served by an EIS for beneficial impacts is informing and involving the public in agency decisions, yet that argument fails as well.

3. Requirement for Public Participation

The argument an *EIS* for beneficial impacts is required because of the need for public participation fails at the outset. All agency actions not covered by a CATEX or exempt from NEPA compliance require at least an EA. An EA is still a document available to the public and generally allows for public comment. While courts do not agree on the level of public participation required for an EA, it is important to note no court has held an EIS needs to be prepared simply because it provides enhanced opportunities for public involvement. For this argument to succeed, all EAs would have to be invalidated categorically. Such a position is contrary to the intent of NEPA and CEQ's interpretation and is simply not legally supportable. Nevertheless, this section will address the argument and demonstrate that from a policy perspective, an EIS is not required for beneficial significant effects, due to an argument based on the need for public participation.

As discussed above, very little is said in the statute or the legislative history about how *much* public participation should be required in the NEPA process. It is possible that Congress intended to limit public participation to information sharing, particularly the results of studies, in order to further research into enhancing the

[267] Implementation of Procedural Provisions of NEPA, 43 Fed. Reg. at 55,979.

environment and limiting pollution.[268] It is also possible, to the extent Congress intended public participation, they may have only intended it for projects determined to have a significant adverse effect on the environment, as NEPA only discusses one environmental statement.[269] Whatever was intended, the regulations promulgated by CEQ require substantial public participation in the drafting of an EIS, beginning with the publication of a notice to prepare the EIS, soliciting comments on scoping and then the draft, and even holding public hearings when appropriate.[270] The requirement for public participation in drafting an EA is less well defined, but still includes information sharing and, in most cases, opportunities for public comment. Considering the statements in the legislative history and the statute, these procedures set out in the regulations for public notification and involvement in the EA process are more than sufficient to satisfy this purpose of NEPA.

Implementation of public participation for an EA is varied, and courts disagree as to exactly what is required. Early NEPA cases required the government to provide enough information for the public to evaluate the environmental factors that influenced the agency decision, and then required that information from the public be able to flow back to the government.[271] Since the 1978 regulations, some courts have required that when an EA is used as the basis of a decision, it must be made available to the public for the full 45 day comment period, the same as an EIS.[272] But not all courts agree. Some have declined to require that EAs be made available for public comment in all cases prior to final agency decisions.[273] Much like the courts, the regulations have two requirements for public participation: A requirement environmental information be made available to the public and public officials,[274] and a requirement to "solicit appropriate information from the public."

Not surprisingly, agency approaches to public participation in EAs vary. Some agencies mirror the process for an EIS, while others just make the EA and a draft FONSI available to the public.[275] The regulations do not specify the exact amount of public involvement required and merely direct agencies to involve the public to the extent practicable.[276] Even so, in most cases, agencies provide some opportunity for public feedback prior to drafting an EA, and then allow comments after a draft EA is produced and before a final EA is issued.[277] Examining all agency

---

[268] *See, e.g.*, 42 U.S.C. § 4332(G).

[269] *Id.* § 4332(C).

[270] *See* 40 C.F.R. §§ 1501.7, 1502.19, 1503, 1506.6.

[271] Ferlo, et al, *supra* note 2, at 122.

[272] *See* Save Our Ecosystems v. Clark, 747 F.2d 1240, 1247 (9th Cir. 1984).

[273] *See* Greater Yellowstone Coalition v. Flowers, 359 F.3d 1257, 1279 (10th Cir. 2004) (citing Pogliani v. U.S. Army Corps of Engineers, 306 F. 32 1235, 1238-39 (2d Cir. 2002)).

[274] *See* 40 C.F.R. § 1500.1.

[275] CEQ, A Citizen's Guide to NEPA Having Your Voice Heard 12 (2007).

[276] 40 C.F.R. § 1501.4 (2012).

[277] Ferlo, et al., *supra* note 268, at 138.

public participation regulations is far beyond the scope of this article, but the Department of Defense (DoD) provides an example of how public participation for an EA is actually handled.

Within the DoD, the EA and FONSI are generally considered public documents and are available for review.[278] Both the Army and Navy requirements mimic the CEQ regulations, pointing out how important public participation is and requiring that the public be involved to the extent practicable.[279] The Air Force provides more detail on how public participation for routine EAs is to be handled by the Environmental Planning Function (EPF). The Air Force regulations require in pertinent part:

> The EPF must make the EA and unsigned FONSI available to the affected public and provide the EA and unsigned FONSI to organizations and individuals requesting them and to whomever the proponent or the EPF has reason to believe is interested in the action, unless disclosure is precluded for security classification reasons.[280]

The regulations then allow for a flexible comment period depending on the magnitude of the action.[281] While the agency is given latitude to adopt an appropriate comment timeframe, the regulations never mention less than a 30-day comment period.[282] Environmental documents are provided to interested parties free of charge and the public is given an opportunity to express concerns and shape the project prior to a decision being made.[283]

This process is not unique to the Air Force or DoD. It is merely an example of how the NEPA process for an EA satisfies a recognized purpose of public participation, that of providing information to the public and allowing information from the public to flow back to the government. Because the EA process satisfies NEPA's purpose of NEPA, even from a policy perspective, the only remaining public participation argument for an EIS over an EA is simply that an EIS is needed because it provides more information and more detailed analysis. To analyze this argument, it is useful to look at the history and development of the EA.

Looking back at the history of NEPA and given the scarce direction in the statute itself regarding providing information to the public, the courts drastically influenced agency approaches to environmental analysis and documents. In early

---

[278] Classified portions of environmental documents are not made available for public review. *See* 32 C.F.R. §§ 775.11, 775.5 (2012); 32 C.F.R. §§ 651.36, 651.13 (2012); 32 C.F.R. § 989.15, 989.26 (2012).

[279] *See* 32 C.F.R. § 775.11; 32 C.F.R. § 651.36.

[280] *Id.* § 989.15.

[281] *Id.*

[282] *Id.*

[283] *Id.*

cases, courts found enough fault with the contents of EISs that many agencies began to include as much information as possible in their analysis so that they could not be challenged in litigation.[284] While this approach might produce a comprehensive document, it undermined NEPA's goals, as the documents became too large and too full of extraneous information to be readily useful in identifying the environmental effects and best approach for a project.[285] In large part, the 1978 regulations were created to deal with the increasing problem of environmental documents becoming so large and bulky that they were of little use to the public or to decision-makers.[286] While the purpose of providing information to the public was being met, at least in name, these large documents may have actually been detrimental to the true purpose of public education and participation.[287]

President Carter observed: "But to be more useful to decision-makers and the public, environmental impact statements must be concise, readable and based upon competent, professional analysis. They must reflect a concern with quality, not quantity. We do not want impact statements that are measured by the inch or weighed by the pound."[288] With this direction, CEQ drafted the 1978 regulations with, as noted above, the goals of saving time, reducing paperwork and producing better decisions.[289] It should not have been surprising that CEQ even specified how long a typical EIS should be. According to the regulations, a final EIS should ". . . normally be less than 150 pages and for proposals of unusual scope or complexity shall normally be less than 300 pages."[290] CEQ further included a provision that for lengthy statements, just the summary could be circulated with the full document available on request.[291] Presumably, it was the position of CEQ that a summary of the EIS was sufficient in many cases to fulfill the NEPA purpose of providing information to the public.

No data is available to show just how much impact these page limits had on the preparation of an actual EIS, but a CEQ report from 2003 indicated that a typical EIS would "range from 200 to more than 2,000 pages in length," and "require 1 to more than 6 years to complete."[292] Conversely, an EA can be produced quickly, from a few weeks to 18 months, depending on the project and its complexity.[293] A typical EA for a small project is also usually only about 10 to 30 pages, or 50 to

---

[284] *See* FERLO, ET AL., *supra* note 3 at 14. Squillace (citing Exec. Order No. 11991 (1977)).

[285] FERLO, ET AL., *supra* note 3 at 14.

[286] FERLO, ET AL., *supra* note 3 at 13.

[287] FERLO, ET AL., *supra* note 3 at 13.

[288] FERLO, ET AL., *supra* note 2 at 14 (citing CEQ, The President's Environmental Program, M-12 (1977)).

[289] Implementation of the Procedural Provisions of NEPA 43 Fed. Reg. at 55978.

[290] 40 C.F.R. § 1502.7.

[291] *Id.* § 1502.19.

[292] Task Force Report, *supra* note 12, at 66.

[293] Task Force Report, *supra* note 12, at 66.

200 pages for a more complicated project.[294] Because CEQ guidance states a normal EIS should be less than 150 pages, and in many cases, the summary of the EIS is sufficient to meet the requirement of informing the public, it is hard to argue more information is needed than what is already found in an EA that could easily rival the size of what an EIS was intended to be.

Assuming the EA has met its burden of providing quality analysis, it also provides the amount of information that is necessary "to show why more study is not warranted."[295] Accordingly, it would satisfy the public information requirement under the CEQ regulations, even for an EIS. It would also meet the purposes outlined in the statute and discussed in the legislative history. A project with no adverse impacts does not require a multi-volume, multi-million dollar document to assess the context and intensity of the beneficial impacts, or to provide over-analysis of which beneficial alternative is the most beneficial.

"Ultimately, of course, it is not better documents but better decisions that count. NEPA's purpose is not to generate paperwork—even excellent paperwork—but to foster excellent action."[296] Arguably, for an action with only beneficial impacts, the policies in NEPA have already done this, by providing direction to agencies to engage in this type of activity. Requiring an EIS for such an action is not in keeping with any of the purposes of NEPA, and serves only to frustrate the goals of the Act

E. Functional Equivalence

The doctrine of functional equivalence bears discussing not for its own sake, but because it illustrates a general interpretation of NEPA by the courts, and arguably, even Congress. The most cited case for the creation of the functional equivalence doctrine came out of the D.C. Circuit in 1973.[297] The controversy was over the promulgation of a new source performance standard by EPA.[298] EPA published proposed standards in 1971, with final regulations and additional justification for them following in 1972.[299] The standards and regulations were issued without preparing an EIS.[300] The time table for adoption of new standards only allowed a total of 210 days from proposal to adoption.[301] Accordingly, it would have been possible for the court to conclude that preparation of an EIS was not possible. Instead, the court found that EPA was exempt from NEPA compliance for promulgation of

[294] Task Force Report, *supra* note 12, at 66.

[295] 40 C.F.R. § 1502.2.

[296] *Id.* § 1500.1.

[297] *See* Mandelker, *supra* note 29, § 5:15 (citing Portland Cement Assoc. v. Ruckelshaus, 486 F.2d 375 (D.C. Cir. 1973)).

[298] *Portland Cement Assoc*., 486 F.2d at 378.

[299] *Portland Cement Assoc.*, 486 F.2d at 379.

[300] *Id.*

[301] *Id.* at 380-81 (citing 42 U.S.C. § 1857c-6(b)(1) (1972).

new source standards, because the process that EPA went through to produce those standards was functionally equivalent to the NEPA EIS process.[302]

The court also discussed a broader exemption for all actions taken by the EPA.[303] While not actually ruling on that issue, the D.C. Circuit set out several factors for consideration, two of which are relevant to this discussion:

> (1) An exemption from NEPA is supportable on the basis that this best serves the objective of protecting the environment which is the purpose of NEPA . . . (4) An impact statement requirement presents the danger that opponents of environmental protection would use the issue of compliance with any impact statement requirement as a tactic of litigation and delay.[304]

The court did not ultimately conclude that EPA was exempted from NEPA compliance for all actions, but presumably these factors weighed into the decision to exempt the promulgation of new source performance standards.[305]

The rule-making procedures arguably provided the equivalent of the public participation requirement of NEPA. The court also seemed to rely on EPA's function of protecting the environment, concluding that NEPA's purpose was similarly to protect the environment. The court reasoned:

> EPA's proposed rule, and reasons therefor, are inevitably an alert to environmental issues. The EPA's proposed rule and reasons may omit reference to adverse environmental consequences that another agency might discern, but a draft impact statement may likewise be marred by omissions that another agency identifies. To the extent that EPA is aware of significant adverse environmental consequences of its proposal, good faith requires appropriate reference in its reasons for the proposal and its underlying balancing analysis.[306]

Subsequent to this ruling, Congress statutorily exempted actions taken under the Clean Air Act (CAA) from compliance with NEPA section 102, by amendments to the CAA in 1974.[307]

---

[302] *Portland Cement Assoc.*, 486 F.2d at 386-87.

[303] *Id.* at 383-84.

[304] *Id.*

[305] *Portland Cement Assoc.*, 486 F.2d at 383-84.

[306] *Id.* at 386.

[307] 15 U.S.C. § 793 (2013).

Prior to the D.C. Circuit's decision and the amendments to the CAA, Congress had already exempted certain actions under the Federal Water Pollution Control Act (FWPCA).[308] This exemption reads:

> Except for the provision of Federal financial assistance for the purpose of assisting the construction of publicly owned treatment works as authorized by section 1281 of this title, and the issuance of a permit under section 1342 of this title for the discharge of any pollutant by a new source as defined in section 1316 of this title, no action of the Administrator taken pursuant to this chapter shall be deemed a major Federal action significantly affecting the quality of the human environment within the meaning of the National Environmental Policy Act of 1969.[309]

As the D.C. Circuit highlighted, "the debate of a later Congress [has] been described by the Supreme Court as offering a hazardous basis for inferring the intent of the earlier Congress."[310] When looking at this exemption and the exemption for actions under the CAA, they have one striking thing in common: the exempted actions are ones that will presumably *benefit* the environment.

The promulgation of new source standards under the CAA is designed to effectuate the reduction of air pollution "through the application of the best system of emission reduction which . . . the Administrator determines has been adequately demonstrated."[311] Other actions under the CAA, such as designating criteria pollutants or setting ambient air quality standards, also are designed to benefit the environment. Likewise, the exempted portions of the FWPCA are designed to reduce and limit water pollution. The two actions specifically not exempt from NEPA compliance are the construction of new treatment facilities and the permitting of new pollutant sources.[312] Construction of a treatment facility could obviously have adverse environmental impacts, depending on the location and size of the facility. Permitting a new pollutant source also presents a very real danger of adverse environmental impacts. In fact, some adverse impact is almost guaranteed. By providing these exemptions from NEPA compliance, Congress appears to be interpreting NEPA to require an EIS for adverse actions and exempting actions that are designed to benefit the environment. It is very difficult to argue that the CAA and the FWPCA have not had, and continue to have, beneficial significant effects on the environment.

---

[308] An Act to Amend the Federal Water Pollution Act, P.L. 92-500, 86 Stat. 816 (1972).

[309] 33 U.S.C. § 1371(c) (2013).

[310] *Portland Cement Assoc.*, 486 F.2d at 315 (citing United States v. Sw. Cable Co., 392 U.S. 157, 170 (1968)).

[311] *Portland Cement Assoc.*, 486 F.2d at 378 (quoting 42 U.S.C. § 7411(a)(1) (2013)).

[312] 33 U.S.C. § 1371(c).

The functional equivalence exemption has also been held to apply to EPA's actions under other statutes that have no subsequent exemption by Congress, including the Federal Insecticide, Fungicide and Rodenticide Act (FIFRA), the Safe Drinking Water Act, the Resource Conservation and Recovery Act and the Clean Water Act (CWA).[313] A full discussion of the functional equivalence doctrine is beyond the scope of this article, but two cases highlight how courts have interpreted this exemption as consistent with the interpretation of NEPA requiring an EIS only for significant adverse impacts. These two cases come from the Ninth Circuit and the Tenth Circuit.

In 1975, the Tenth Circuit addressed an order from the EPA Administrator suspending the registration of certain pesticides under FIFRA.[314] The administrator did so without producing an EIS.[315] Ultimately the court concluded that the report produced by EPA studying the problem was sufficient to comply with NEPA.[316] In doing so, the court reasoned:

> Furthermore, the substance of NEPA is such as to itself exempt EPA from the requirement of filing an impact statement. Its object is to develop in the other departments of the government a consciousness of environmental consequences. The impact statement is merely an implement devised by Congress to require government agencies to think about and weigh environmental factors before acting. Considered in this light, an organization like EPA whose regulatory activities are necessarily concerned with environmental consequences need not stop in the middle of its proceedings in order to issue a separate and distinct impact statement just to be issuing it. To so require would decrease environmental protection activity rather than increase it.[317]

In this analysis, the Tenth Circuit embraced the interpretation of NEPA recognized two decades later by the Sixth Circuit in *Friends of Fiery Gizzard v. Farmers Home Admin*. NEPA is designed to empower and direct agencies to consider environmental impacts and ultimately take less harmful actions, not inhibit beneficial action.

In 1992, the Ninth Circuit addressed a claim that EPA and the U.S. Army Corps of Engineers failed to comply with NEPA by entering into a memorandum of agreement as to guidelines for dredge and fill permits.[318] Arguably, the 1972 exemption discussed above and created by the amendment to the FWPCA, exempted

---

[313] *See generally* MANDELKER, *supra* note 29, § 5:15; FERLO ET AL., *supra* note 3, at 245-47.

[314] *See* State of Wyo. V. Hathaway, 525 F.2d 66 (10th Cir. 1975).

[315] *Id.* at 66-67.

[316] *Id.* at 72-73.

[317] *Hathaway*, 525 F.2d. at 71-72.

[318] Municipality of Anchorage v. United States, 980 F.2d 1320, 1322 (9th Cir. 1992).

EPA's action in the case.[319] Ultimately, however, the court did not rule on that issue, instead finding that the obligations of EPA and the Corps are functionally equivalent to those imposed by NEPA.[320] The court noted:

> The purpose of NEPA is to ensure that federal agencies consider the environmental impact of their actions. Under the CWA, Congress has charged the Administrator of the EPA with the duty of cleaning up the nation's navigable waters. We are convinced that in the circumstances of this case an exemption from NEPA will facilitate the EPA's efforts to clean up the nation's waters . . . .[321]

Essentially, the Ninth Circuit has recognized that the purposes of NEPA and the CWA would not be served by requiring an EIS in situations where doing so would be adverse to the ultimate beneficial environmental outcome. In rejecting the plaintiffs' argument against the exemption, the court stated:

> [Plaintiffs] would have us hold that the EPA, the agency charged with protecting the environment, has violated NEPA, a statute designed to ensure that environmental considerations are weighed appropriately before federal agencies act, by interpreting its guidelines in a manner that is too protective of the environment. Because such a reading skews the logical intent of the statutes, we reject it.[322]

Just like the Tenth Circuit, the Ninth Circuit has embraced the idea that NEPA was enacted to prevent and eliminate environmental degradation and using the statute to prevent beneficial actions is counter-productive.

This article does not argue that agencies should be exempt from NEPA compliance for actions with only beneficial consequences. Any actions not categorically excluded would still require an EA. However, the development of the functional equivalence doctrine, especially the exemptions provided by Congress, demonstrate that NEPA is consistently interpreted as being primarily concerned with actions that have adverse consequences for the environment. An interpretation that would require an agency to produce an EIS ". . . just to be issuing it . . .,"[323] would ". . . [skew] the logical intent of the statute . . .,"[324] and should therefore be rejected.

---

[319] *Id.* at 1327-28.

[320] *Id.* at 1329.

[321] *Id.*

[322] *Municipality of Anchorage*, 980 F.2d at 1329.

[323] *Hathaway*, 525 F.2d at 72.

[324] *Municipality of Anchorage*, 980 F.2d at 1329.

F. The Correct Resolution of the Circuit Split

When the Eleventh Circuit held that an SEIS was required for changes to a project that resulted in only beneficial impacts, the holding necessarily meant that an EIS for projects with beneficial significant impacts was required as well, since the standard for when an SEIS is required is the same as the standard for when an EIS is required.[325] This holding was based on a case from the Fifth Circuit which, while appearing to support exactly the conclusion drawn by the Eleventh Circuit, later disavowed such an interpretation.[326] Neither the Fifth Circuit nor the Eleventh Circuit provided any analysis of the regulations promulgated by CEQ in 1978, and which the U.S. Supreme Court had already determined were due substantial deference.[327] It wasn't until the Sixth Circuit addressed the issue in 1995 that an analysis relied upon the current regulations promulgated by CEQ. The Sixth Circuit looked at the regulations and definitions to correctly conclude that NEPA, as interpreted by CEQ and implemented by the CEQ regulations, did not intend for agencies to have to prepare an EIS for projects with only beneficial significant impacts.[328]

The legislative history and the text of the bill originally proposed by the Senate demonstrate that what is actually required in an EIS is a discussion of the overall environmental impacts of the project, with special attention paid to the significant adverse environmental effects which cannot be avoided under any alternative.[329] The highlighted requirement for discussion of alternatives in the final law, combined with a requirement to discuss adverse impacts which cannot be avoided, creates a process very similar to the original text from the Senate bill.[330] The original bill focused on requiring the avoidance of adverse impacts and justifying those that could not be avoided.[331] In the final version, the alternatives analysis simply provides a way to discuss mitigation and avoidance of those impacts identified in subsection (i), while subsection (ii) requires notice of any adverse impacts which cannot be avoided or mitigated.[332]

Both the Chair of CEQ and President Obama have recently emphasized that "NEPA was enacted to promote efforts that will prevent or eliminate damage to the environment . . . ."[333] This has been the focus of NEPA since the beginning. NEPA was drafted and enacted to prevent continued environmental degradation, not prevent environmental enhancement. The CEQ regulations were drafted to promote

[325] *See supra* Part III.A.

[326] *See supra* Part III.A.1.

[327] *See supra* Part III.A.; *Andrus*, 442 U.S. at 357.

[328] *See supra* Part III.A.4.

[329] *See supra* Part III.B-C.

[330] 42 U.S.C. § 4332(C).

[331] S. Rep. No. 91-296, at 2.

[332] 42 U.S.C. § 4332(C).

[333] Proclamation No. 8469, 75 Fed. Reg. 885-886; Sutley Memorandum, *supra* note 180, at 2.

better decisions while reducing paperwork and time. Requiring an EIS for actions with only beneficial significant impacts will not result in an environmentally better decision. Instead, if requiring an EIS for projects with only beneficial impacts does not kill the project outright, it will result in multi-year delays and millions of dollars in additional cost. The correct interpretation of NEPA is therefore is that an EIS is not required for actions with only beneficial significant impacts.

The REPI project at Fort Benning is a perfect example of the kind of project NEPA may have envisioned 44 years ago. With NEPA's stated policy of the federal government to "create and maintain conditions under which man and nature can exist in productive harmony . . . ,"[334] this project seems to be the embodiment of the spirit of NEPA. By restoring and preserving the pine forest, the project at Fort Benning is doing exactly what NEPA calls for—creating and maintaining "conditions under which man and nature can exist in productive harmony . . .,"[335] ensuring military training can continue by avoiding conflicting development, and restoring and protecting natural habitat for endangered species and public enjoyment.

There are only a very limited number of EISs filed each year by federal agencies. In 2009, across the entire federal government, there were only 450.[336] The fact this is such a small percentage of the hundreds of thousands of federal actions is both a testament to how well NEPA has worked at minimizing the environmental impacts of the government, and an indication of how assiduously agencies avoid projects with the costs associated with an EIS. Agency budgets are only so large, and have become smaller with the unexpected effects of sequestration.[337] When an agency has to prioritize its actions, at a time when it is also making decisions about furloughing employees, agency actions like the REPI project at Fort Benning are not going to make the cut if the agency has to shoulder the additional costs associated with an EIS. Many projects that result in only beneficial impacts are simply not going to be vital enough to the function of the agency to justify the cost. Such projects will not be funded, or at best, all beneficial environmental effects will be avoided. Interpreting NEPA to require an EIS for this type of project turns the act on its head, effectively creating a situation where the environment must be saved from an act that was designed to protect it. Such an interpretation cannot be, and is not, correct.

## IV. A SUGGESTED AGENCY APPROACH

No matter how well reasoned, sensible, and correct the argument that no EIS is required for actions with only beneficial impacts, it would be naïve to expect

---

[334] 42 U.S.C. § 4331.

[335] *Id*.

[336] Council on Environmental Quality, Environmental Quality, Calendar Year 2009 Filed EISs, http://ceq.hss.doe.gov/nepa/Calendar_Year_2009_Filed_EISs.pdf.

[337] *See* Zients Letter, *supra* note 13.

that no group would raise the argument if such an argument stood to benefit the group's position in a dispute. Since funding for litigation is not unlimited on either side, the best way to prevent such an argument from being raised is to be clearly prepared to defeat it. With that in mind, agencies can and should take steps to be ready to handily defeat this argument.

The best solution from the perspective of an agency would be, of course, for Congress to amend NEPA, clearly stating that only significant *adverse* impacts on the environment trigger the EIS requirement. However, given that NEPA has remained virtually unchanged for 44 years, this solution seems unlikely. Almost as good a solution would be for CEQ to add back into the regulations the 1973 language, specifying that impacts must be adverse to trigger the need for an EIS.[338] Yet these regulations also have remained virtually unchanged since they were published in 1978. Any change at this point seems unlikely.

The best option left for an agency is to amend their own regulations to ensure an agency may rely on these for an interpretation that an EIS is not required for actions with no significant adverse impacts. It may be tempting to simply rely on CEQ regulations, arguing that the appropriate interpretation is that set out in Part III.D of this article, the same interpretation reached by Sixth Circuit.[339] Such an argument would hopefully be persuasive, but there is no guarantee that the court would accept it. Furthermore, as CEQ will not be there arguing the case, the court may well afford no deference to the agency's interpretation of NEPA.[340] Accordingly, relying on the CEQ regulations will not foreclose the issue. However, by amending their own regulations to set out the interpretation clearly, an agency would be entitled to substantial deference in the interpretation of its own regulations.[341] While agency NEPA regulations are somewhat unusual in the context of agency deference for implementing regulations, agencies are nevertheless entitled to this deference.[342]

In *Chevron, U.S.A. Inc. v. National Resources Defense Council, Inc.*, the U.S. Supreme Court established two rules for determining if an agency's interpretation of a statute it administers is entitled to deference.[343] First, the court must determine if the language at issue is ambiguous, for if Congress has clearly spoken to the issue,

---

[338] *See* Preparation of Environmental Impact Statements: Guidelines, 38 Fed. Reg. at 20,552 (regulation clarifying to have significant impact, must be adverse effect on human beings).

[339] *See Friends of Fiery Gizzard*, 61 F.3d at 501.

[340] *See* Grand Canyon Trust v. F.A.A., 290 F.3d 339, 341-42 (D.C. Cir. 2002).

[341] *See* Auer v. Robbins, 519 U.S. 452, 461 (1997); Bowles v. Seminole Rock & Sand Co., 325 U.S. 410, 413-14 (1945).

[342] *See, e.g.*, Ohio Valley Envtl. Coal. v. Aracoma Coal Co. 556 F.3d 177, 193-94 (4th Cir. 2009) (court held Corps regulations implementing NEPA entitled to highly deferential review, or Auer Deference); Sylvester v. U.S. Army Corps of Engineers, 884 F.2d 394, 399 (9th Cir. 1989) (court held Corps' NEPA regulations entitled to deference).

[343] Chevron, U.S.A. Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837, 842-43 (1984).

then there can be no interpretation other than the one Congress has directed.[344] If the statute is silent or ambiguous, on the other hand, then the reviewing court must defer to an agency's interpretation, if that interpretation is based on a permissible construction of the statute.[345] As the Second Circuit noted, NEPA's language "has been characterized as 'opaque' and 'woefully ambiguous' . . . ."[346] Certainly, NEPA has failed to define "significantly," in terms of what exactly is meant by "significantly affecting the quality of the human environment."[347]

NEPA is unusual though, in that no single agency implements the Act. Each agency is responsible for complying with NEPA and preparing its own environmental impact statements and assessments as appropriate. In analyzing compliance with acts that similarly apply to multiple agencies, some courts have concluded no single agency's interpretation of a statute is controlling, and thus entitled to deference.[348] Yet unlike some acts, such as the Freedom of Information Act, where no single agency oversees implementation of that law, NEPA also created CEQ, which *is* a single agency with authority to interpret NEPA. Early on, the U.S. Supreme Court held that CEQ's interpretation of NEPA, and the regulations promulgated by CEQ, were entitled to substantial deference.[349] CEQ *has* offered a definition of "significantly," although that definition also fails to address whether beneficial effects alone qualify under that definition.[350] Had CEQ clearly provided an answer as to whether beneficial effects alone can qualify as a significant effect, the analysis would be over. Unfortunately, while it is possible to ascertain an answer, as discussed in part III.D of this article, CEQ did not set that answer out clearly.

CEQ is entitled to deference in the interpretation of its regulations, but other agencies may not be. The D.C. Circuit is the only Circuit to squarely address the issue of whether agencies are entitled to deference in their interpretation of CEQ regulations since the publication of the 1978 regulations. The D.C. Circuit has recognized that while agencies are entitled to deference in the interpretation of their *own* regulations, including their NEPA implementing regulations,[351] agencies are entitled to no deference in the interpretation of NEPA or CEQ's implementing regulations.[352] Other circuits have not addressed the issue of interpreting CEQ regula-

---

[344] *Id.*

[345] *Id.*

[346] *Hanley*, 471 F.2d at 823 (quoting City of New York v. United States, 337 F. Supp. 150, 159 (E.D.N.Y. 1972); Larry H. Voight, *The National Environmental Policy Act and the Independent Regulatory Agency*, 5 Nat. Resources Law. 13 (1972)).

[347] 42 U.S.C. § 4332(C).

[348] *See, e.g.*, Al-Fayed v. C.I.A. 254 F.3d 300, 307 (D.C. Cir. 2001) (holding that because the Freedom of Information Act applies across all federal agencies and no single agency administers the Act, a single agency interpretation is not entitled to deference).

[349] Andrus, 442 U.S. at 357.

[350] *See* 40 C.F.R. § 1508.27; *see also supra* Part III.D.

[351] *Grand Canyon Trust*, 290 F.3d at 341-42.

[352] *Id*.

tions quite as squarely, but some have been more generous in upholding what could be characterized as an agency interpretation of NEPA based on agency regulations.

The Ninth Circuit has applied the very deferential *Chevron* test to the Army Corps of Engineers interpretation of NEPA and agency regulations.[353] In that case, the Corps was interpreting its regulations to define the scope of what ultimately would be subject to environmental analysis.[354] The development project which was the subject of the dispute included skiing facilities, a resort village and a golf course.[355] The Corps was involved because a permit was required for the filling of wetlands in the area where the golf course was to be located.[356] No other portion of the project required a permit from the Corps or any other form of Corps involvement.[357] Interpreting their own agency regulations, the Corps determined that they should limit their NEPA analysis to the golf course, as that was the extent of the Corps' agency action.[358] Mr. Sylvester disagreed and filed suit.[359] In applying the *Chevron* test for deference, the Ninth Circuit held:

> First, the court must follow any unambiguously expressed intent of Congress . . . . Second, when a statute is 'silent or ambiguous' with respect to a specific issue, the court must defer to the agency's interpretation if based on a permissible construction of the statute . . . . When we apply these rules to the facts, we find no clear intention in the NEPA with respect to the proper resolution of the issue before us. Moreover, we cannot say that the Corps' interpretation is an impermissible reading of the statute. We hold, therefore, that the district court should have deferred to the Corps' regulations as approved by the CEQ.[360]

Arguably, the Ninth Circuit has allowed the Corps to not only interpret their own regulations but NEPA as well. The court appears to grant the Corps the same deference as if the interpretation had come from CEQ. Such an approach makes sense when one follows the Ninth Circuit's reasoning:

> [T]he CAA requires the EPA to review the Corps' regulations and designates the CEQ as the arbitrator in disputes between federal agencies on environmental issues . . . . This is not done as an idle exercise. It is to provide guidance to all who may be concerned,

---

[353] *Sylvester*, 884 F.2d at 394.

[354] *Id.*

[355] *Sylvester*, 884 F.2d at 396.

[356] *Id.* at 396-97.

[357] *Id.*

[358] *Id.*

[359] *Id.*

[360] *Sylvester*, 884 F.2d at 399 (citing *Chevron, U.S.A. Inc.*, 467 U.S. at 842-43).

> including courts. Thus, even though the Corps actually promulgated the regulations, we believe that the principles underlying *Chevron* entitle them to, and require us to extend, deference.[361]

The Ninth Circuit essentially concluded even though the Corps promulgated the regulations, the fact those regulations had to be reviewed and approved by EPA and CEQ entitled the Corps regulations to as much deference as CEQ regulations in their interpretation of NEPA.[362]

The Ninth Circuit appears to be on one end of the deference spectrum, while the D.C. Circuit is on the other end, with other circuits falling somewhere in between. However, all circuits that have addressed the issue agree that agency interpretations of their own regulations, even regulations implementing NEPA, are entitled to substantial deference.[363] Accordingly, an agency's best option to minimize litigation risk is to set out clearly in its own regulations that in order for an action to trigger the need for an EIS, it must have a significant *adverse* effect on the quality of the human environment. Courts would have great difficulty in reaching compelling a contrary conclusion if the requirement for a significant adverse effect to be present is set out in an agency regulation, approved by CEQ.

## V. CONCLUSION

While at least one circuit has interpreted NEPA to require an agency to prepare an EIS for actions with only beneficial significant effects, that interpretation of NEPA is not consistent with the purposes of the Act, or the Act's legislative history. NEPA was enacted, in part, to empower and direct the government to deal more effectively with growing environmental problems. It was not intended to be a roadblock to agency actions that actually serve to enhance the human environment. While actions that have both adverse and beneficial effects require an EIS, actions with no significant adverse effects should not. Requiring agencies to prepare an EIS for actions with no significant adverse effects will frustrate the purposes of NEPA, causing agencies to abandon projects that might have benefited the environment, or at the very least, cause agencies to avoid the beneficial effects that could have resulted from their actions.

---

[361] *Sylvester*, 884 F.2d at 399 (citing 42 U.S.C. §7609(a)-(b) (1989)).

[362] *Sylvester*, 884 F.2d at 399.

[363] *See Ohio Valley Envtl. Coal*, 556 F.3d at 193-94 (court held Corps is entitled to substantial deference in interpreting its own NEPA implementing regulations); Utah Envtl. Cong. v. Dale Bosworth, 443 F.3d 732, 742-43 (10th Cir. 2006) (court held agency's interpretation of its own categorical exclusion regulation entitled to substantial deference); Mississippi River Basin Alliance v. Westphal, 230 F.3d 170, 175 (5th Cir. 2000) (court held CEQ regulations and the Corps entitled to substantial deference); Iowa Citizens for Envtl. Quality, Inc. v. Volpe, 487 F.2d 849, 855 (8th Cir. 1973) (court held Federal Highway Administration's administrative interpretation of NEPA entitled to great deference).

Opponents to an agency action will inevitably raise the argument an EIS is required for *any* significant effect. To that end, the best defense an agency can muster is to amend its own regulations to set out clearly that no EIS is required when the action has no significant adverse impacts. Such an inclusion in agency regulations is supported by the legislative history of the act, the previous versions of the CEQ regulations, and the preamble to the implementing regulations. Both President Obama and the Chair of CEQ have recently noted that the purpose of NEPA is to "prevent or eliminate damage to the environment . . . ."[364] CEQ has also wisely noted that NEPA procedures, including those for the production of an EIS, must further the purposes of the Act, "otherwise they are indeed useless paperwork and wasted time."[365] By setting out in agency regulations that an action must have a significant *adverse* effect in order to trigger the need for an EIS, agencies can avoid wasted time and resources and further the goals of NEPA by engaging in projects that benefit the environment. For if NEPA is interpreted to require an EIS for projects with beneficial significant impacts, there may not be sufficient funding or time to complete them.

[364] Proclamation No. 8469, 75 Fed. Reg. 885-886; Sutley Memorandum, *supra* note 180, at 2.

[365] Implementation of Procedural Provisions of NEPA, 43 Fed. Reg. at 55,979.

# NON-GOVERNMENTAL EMPLOYEES' PERSONAL CONFLICTS OF INTEREST IN PUBLIC ACQUISITION: A CASE FOR GREATER HARMONIZATION

*Major Garrett Jonathan Bruening**



* Maj Garrett J. Bruening, Judge Advocate, United States Air Force (LL.M., Government Procurement Law, The George Washington University Law School (2013); J.D., The University of South Dakota School of Law (2006); M.B.A., The University of South Dakota School of Business (2004); B.S.B.A, The University of South Dakota School of Business (2003)) is an acquisition attorney at the Research and Specialized Contracting Branch, Air Force Materiel Command Law Office, Wright-Patterson Air Force Base, Ohio. This article is derived from a thesis submitted in partial satisfaction of the requirements for the degree of Master of Laws in Government Procurement at The George Washington University Law School. The views expressed in this paper are solely those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense or U.S. Government.

LIST OF FIGURES

## I. INTRODUCTION

Integrity is central to public administration.[1] Integrity is especially central to public acquisition.[2] Public systems promoting integrity must both minimize the opportunities for deviation from the public's objectives and maximize the public's ability to correct any occurring deviations.[3] As integrity systems mature and develop, they churn and reinvent themselves. Old law guarded against the issues of its day. New issues drove new law. New law changed old law. But in that churning process, sometimes the issues the old law guarded against are forgotten. Forgotten, at least, until those same issues emerged again.

---

[1] *See* Exec. Order No. 11,222, §101, 30 Fed. Reg. 6,469, 6,469 (May 8, 1965) ("Where government is based on the consent of the governed, every citizen is entitled to have complete confidence in the integrity of his government. Each individual officer, employee, or adviser of government must help to earn and must honor that trust by his own integrity and conduct in all official actions.").

[2] *See* Steven L. Schooner, *Desiderata: Objectives for a System of Government Contract Law*, 2 Pub. Procurement L. Rev. 103, 103 (2002) (citing integrity as "pillar" in public acquisition). *See also* Christopher R. Yukins, *Integrating Integrity and Procurement: The United Nations Convention Against Corruption and the UNCITRAL Model Procurement Law*, 36 Pub. Cont. L.J. 307, 307 (2007) (arguing for greater integration of anti-corruption international law with the United Nations Commission on International Trade Law Model Law on Procurement of Goods, Construction, and Services). Integrity is especially important in the federal system given the large amount of money moving both out of the market as taxes and back into the market through contracts, grants, and other transactions. The government spent the following billions of dollars contracts and grants in the following fiscal years (format: FYXX, contracts, grants): FY10, $540.0, $614.3; FY11, $539.7, $567.0; FY12, $517.7, $538.6. USASpending.gov, *available at* http://www.usaspending.gov/explore. Money spent on other transaction is discussed separately later.

The paper uses the term "public acquisition" broadly to capture all the means the federal government funds its work through non-federal entities. The most obvious means is contracts wherein the government purchases goods or services for its use. However, the government can accomplishes other work, like basic research, provision of healthcare and education, etc., through grants, cooperative agreements, and other transactions. *See* 31 U.S.C. § 6303 (2013) (directing agencies to use contracts when "the principal purpose of the instrument is to acquire property or services for the direct benefit or use of the United States Government . . . .") (parentheticals omitted); 31 U.S.C. § 6304 (2013) (directing agencies to use grants when "the principal purpose of the relationship is to transfer a thing of value to the State or local government or other recipient to carry out a public purpose of support or stimulation authorized by a law of the United States [and] substantial involvement is not expected between the executive agency and the State, local government, or other recipient when carrying out the activity contemplated in the agreement."); 31 U.S.C. § 6305 (2013) (directing agencies to use cooperative agreements when "the principal purpose of the relationship is to transfer a thing of value to the State, local government, or other recipient to carry out a public purpose of support or stimulation authorized by a law of the United States instead of acquiring . . . property or services for the direct benefit or use of the United States Government [and] substantial involvement is expected between the executive agency and the . . . recipient when carrying out the activity contemplated in the agreement.").

[3] *See* Christopher R. Yukins, *A Versatile Prism: Assessing Procurement Law Through the Principal-Agent Model*, 40 Pub. Cont. L.J. 63,63 (2010) (applying economic agency theory to federal procurement and noting agent controls exists through monitoring and sanctioning measures).

The law concerning conflicts of interest in public acquisition is one such example. From 1863 to 1962, for almost a hundred years, federal law criminalized the conflict itself: one's performance of public acquisition with an entity with which one is financially interested. This law was generally applicable and implied regardless of employer or public acquisition vehicle one worked under.

But then, in 1962, the law changed. Congress widened the field of prohibited personal conflicts applicable to government employees but wholly decriminalized the same activity for everyone else. Thus, overnight, Congress legalized non-government employees recommending the government do business with firms they had a financial interest in, opining about the technical qualifications of said firms, and even selecting said firms for government business when so empowered through their public acquisition vehicle.[4] The law went from wide and thin to narrow and deep.

Since 1962, and especially in modern times, there has been a renewed interest in the conflicts of interest of non-governmental employees[5] as the issues the old law prevented or addressed began to emerge again as their prior restraints had been removed.[6] Agencies working largely independently, and even Congress, re-invented the wheel over and over again through rules, regulations, contract or agreement clauses, and even statutes. A loose patchwork emerged. The most recent remedial patch is FAR Subpart 3.11, Preventing Personal Conflicts of Interest for Contractor Employees Performing Acquisition Functions, and its associated clause, FAR 52.203-16. But it is not the only one.

This article advocates the criminalization of the evil itself: performance of conflicted public acquisition. Doing so would create a common foundation[7]

---

[4] *See generally* Administrative Conference of the United States, Administrative Conference Recommendation 2011-3: Compliance Standards for Government Contractor Employees—Personal Conflicts of Interest and Use of Certain Non-Public Information 10 (2011), *available at* http://www.acus.gov/sites/default/files/documents/Recommendation%202011-3%20%28Contractor%20Ethics%29.pdf (noting that acquisition support and operations & management services present a higher risk of conflicted personal behavior). *But see* Professional Services Council, Review of Regulatory Coverage Regarding Prevention of Personal Conflicts of Interest for Contractor Employees (FAR PCI Comment) at 6, *available at* http://www.regulations.gov/#!documentDetail;D=FAR-2011-0091-0002 (government services trade association contending referenced services do not "per se, raise the risk of" personal conflict of interest).

[5] *See, e.g.,* National Defense Authorization Act for Fiscal Year 2013, Pub. L. No. 112-239, § 829, 126 Stat. 1632, 1841-2 (2013) (directing the Secretary of Defense to determine whether the application of contractor personal conflicts of interest regulations should be expanded); Review of Regulatory Coverage Regarding Prevention of Personal Conflicts of Interest for Contractor Employees (FAR PCI COMMENT), 76 Fed. Reg. 68,046 (Nov. 2, 2011) (requesting public comment on whether FAR Subpart 3.11 should be expanded in coverage or application on the same day FAR Subpart 3.11 was promulgated).

[6] *See* Administrative Conference of the United States, *supra* note 4, at 6. (describing how the outsourcing of federal acquisition functions has driven a need for tighter ethical controls on contractor employees performing those acquisition functions).

[7] *See generally id.* at 8-9 (advocating for a generally applicable personal conflict of interest

upon which the existing disparate systems, to the extent they exist, can either arise toward or, over time churn toward, harmonization. This article does not advocate for particular statutory language. History and the present day give drafters many examples. Some of these are discussed more fully later. Others are found the attached figures found in the appendix. Instead, this article focuses on the central argument itself: why such a law ought to exist.

Part I broadly introduces the article and its central thesis. Part II recounts the development and current state of conflict of interest law and controls. Part II additionally references three figures found in the appendix wherein both current conflict of interest and use of non-public information controls are catalogued. Part III demonstrates why current conflict of interest controls are insufficient to recreate the protection public acquisition enjoyed for almost a hundred years. Part IV addresses some potential arguments against the enactment of the proposed foundational law. Finally, Part V concludes this article.

## II. DEVELOPMENT AND CURRENT STATE OF THE LAW

This part describes how public acquisition conflict of interest law and controls developed and how they apply today. This section will initially demonstrate how the employment statuses intensely relevant to conflict of interest controls on public acquisition today were largely irrelevant for almost a hundred years. Then, will describe how the law fractured and developed to what exists today. Finally, this part will invite the reader to review figures 1, 2, and 3 found in the appendixes. Doing so will both enable the reader to understand how many times the wheel has been reinvented since 1962 and provide the reader an initial starting point for another to advocate for particular statutory language. By the end, the reader should understand the current state of conflict of interest law, appreciate how it came to be so, and have some ideas on what a new law might look like.

### A. Harmonization: 1862–1963

At least as far back as 1863, federal law criminalized certain conflicts of interest in public acquisition regardless of the actor's employment status.[8] This criminal law stated:

> [N]o officer or agent of any banking or other commercial corporation, and no member of any mercantile or trading firm, or person directly or indirectly interested in the pecuniary profits or contracts of such corporation or firm, shall be employed or shall act as an

prohibition to "serve as a floor upon which agencies could build and would not be intended to deter adoption of more expansive ethics regime, either individually or through the FAR Council, to the extent the agencies find it appropriate.").

[8] *See* Act of Mar. 2, 1863, ch. 67, § 8, 12 Stat. 696, 698-9. Codified at Rev Stat § 3490-3494 (1878).

> officer or agent of the United States for the transaction of business with such corporation or firm; and every *such* officer, agent, or member, or person, so interested, who so shall act, shall, upon conviction thereof, be punished . . . .[9]

This criminal law applied to any person functioning as an agent for public acquisition. The law made no distinction in the employment status of the agent: government, contractor, grantee employee, or anything between or outside those statuses, the law viewed all equally and held all equally to the same standard.[10]

In 1909, Congress reworded the statute slightly but left the general thrust intact.

> No officer or agent of any corporation, joint stock company, or association, and no member or agent of any firm, or person directly or indirectly interested in the pecuniary profits or contracts of such corporation, joint stock company, association, or firm, shall be employed or shall act as an officer or agent of the United States for the transaction of business with such corporation, joint stock company, association, or firm. Whoever shall violate the provision of this section shall be [punished].[11]

Between 1909 and the next minor revision in 1948, two reported cases concerned the operation of this law.

The first, *United States v. Strang*,[12] concerned whether a government-owned corporation is an instrumentality of the government. The second, *Rankin v. United States,*[13] concerned whether the government could refuse to pay an implied contract claim from an agent who transacted business on behalf of the government when the agent was financially interested in the transaction. Both demonstrate the type of evils these generally applicable conflict of interest laws sought to thwart.

---

[9] Act of Mar. 2, 1863, ch. 67, § 8, 12 Stat. 696, 698-9.

[10] This law was not the only law concerning conflicts of interest. For various examples, *see, e.g.,* Erwert v. Bluejacket, 259 U.S. 129, 135-7 (1922) (holding public land transaction between Indian and assistant United States attorney void because of statutory prohibition of "trade" between Indians and those "employed in Indian affairs. . . ."); Waskey v. Hammer, 223 U.S. 85 (1912) (federal mining claim surveyor paid by claimants themselves found to be an employee of the government and statutorily prohibited from staking a mining claim); Prosser v. Finn, 208 U.S. 67 (1908) (federal special timber agent held employee of government and statutorily prohibited from purchasing federal lands).

[11] *See* Act of Mar. 4, 1909, Pub. L. No. 60-350, § 41, ch. 321, § 41, 35 Stat. 1088, 1097.

[12] 254 U.S. 491 (1921).

[13] 98 Ct. Cl. 357 (1943).

In *Strang*, the United States charged Mr. James H. Strang and others with violating, and conspiracy to violate, the previously reproduced law.[14] Mr. Strang was an inspector for the Fleet Corporation, the operational arm of the statutorily established United States Shipping Board.[15] Mr. Strang was also a member of the copartnership Duval Ship Outfitting Company (Duval).[16] In February of 1919, Mr. Strang signed and executed three orders to Duval on behalf of Fleet Corporation for repair work on another ship.[17] Once indicted, Mr. Strang moved to dismiss.[18] Mr. Strang argued the Fleet Corporation, as a private corporation organized under the laws of the District of Columbia, was separate and apart from the United States. Prosecutors argued the United States owned all $50M shares of Fleet Corporation and it executed governmental powers originating from statutory law.[19] The Supreme Court held Fleet Corporation "was controlled and managed by its own officers and appointed its own servants and agents who became directly responsible to it. Notwithstanding all its stock was owned by the United States it must be regarded as a separate entity."[20]

*Strang* demonstrates how the proposed law, if at least based in part on prior laws, can naturally fit only public acquisition rather than private acquisition for public purposes. *Strang* shows the fine line between those types of acquisition. When an employee of a traditional prime contractor selects a subcontractor, that employee is not engaging in public acquisition.[21] The prime is "a separate entity."[22] But when the employee is advising (or even obligating) the government to purchase from firm X or writing specifications to favor firm Y, that is public acquisition. *Strang* should help address any concerns about expansive criminal liability.

In *Rankin*, the federal Works Progress Administration (WPA) appointed Mr. John H. Rankin as Director of the Fourth Pennsylvania District.[23] Mr. Rankin was also the long-term lessor of utilized office space on which he was losing money.[24] Mr. Rankin procured bids for WPA office space.[25] Mr. Rankin did not accept any of the submitted bids, instead deciding to sublet his own empty leased office space

---

[14] *See Strang*, 254 U.S. at 492.

[15] *Id*.

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] *Id.* at 493.

[20] *Id.*

[21] Though the line is not as clear when the prime is acting as a lead systems integrator or otherwise providing largely acquisition services.

[22] *Strang*, 254 U.S. at 493.

[23] Rankin v. United States, 98 Ct. Cl. 357, 358 (1943).

[24] *Id. at* 358-9.

[25] *Id.* at 358.

to WPA at the lowest square-footage rate received via the bids.[26] When Mr. Rankin requested payment for his space, the government refused. As no lease had actually been signed,[27] Mr. Rankin sued under implied contract theory.[28] The Court of Claims found Mr. Rankin was clearly an agent for the government in the acquisition of WPA office space and Mr. Rankin had attempted to use the projected federal lease payments to offset a portion of his monthly rent payment obligation.[29] The Court of Claims held that arrangement violated the reproduced above statute and, thus, any implied contract was void.[30]

*Rankin* clearly demonstrates the evil the proposed law seeks to prevent. One may argue that because Mr. Rankin was a government, or special government, employee, his acts would be criminal today[31] and the court would have reached the same result.[32] While that may be true, that argument both misses the larger point and assumes a key fact. The larger point is that it does not require a government employee to engage in conflicted public acquisition. But more importantly, such an argument presupposes Mr. Rankin was a federal employee. Mr. Rankin was appointed "in his individual capacity . . . ."[33] Back then, many persons straddled the line between formal government employee and simple agent of the government. The lines were not as clear then as they can be now. But today, while the lines on paper are clear, the lines in practice are not. *Rankin* is a good example of how a generally applicable law criminalizing conflicted public acquisition could operate outside an 18 U.S.C. § 208 context.

> In 1948, Congress recodified the substance of the 1909 law.
>
> > Whoever, being an officer, agent or member of, or directly or indirectly interested in the pecuniary profits or contracts of any corporation, joint-stock company, or association, or of any firm or partnership, or other business entity, is employed or acts as an officer or agent of the United States for the transaction of business with such business entity, shall be [punished].[34]

---

[26] *Id.* at 360.

[27] Mr. Rankin signed the lease as the lessor but never sent the lease off for counter-signing by the government. *Id*. at 361.

[28] *Id.* at 366-7.

[29] *Id.*

[30] *Id.* at 367.

[31] *See* 18 U.S.C. § 208(a) (2013) (conflict of interest statute for government and special government employees).

[32] *See* 18 U.S.C. § 218 (2013) (allowing agencies to void contracts connected with convictions of 18 U.S.C. § 208).

[33] *Rankin*, 98 Ct. Cl. at 358.

[34] *See* Act of June 25, 1948, Pub. L. No. 80-772, ch. 645, § 434, 62 Stat. 683, 703.

In 1962, this law would be significantly changed to its modern inception as applying only to government employees.[35] But just before the law changed, the Supreme Court decided a case that, like *Rankin*, demonstrated the evils such a law attempted to thwart, and did so. This case is especially helpful here as the Supreme Court gave a very salient analysis of why one's employment status should be irrelevant when guarding against conflicts of interest in public acquisition.

In *United States v. Mississippi Valley Generating Co*.,[36] the Supreme Court affirmed the government's voiding of a contract with the Mississippi Valley Generating Company ("Mississippi Valley") because of a personal conflict of interest arising from a nongovernment employee negotiator and advisor, Mr. Adolph H. Wenzell.[37] Mississippi Valley did not employ Mr. Wenzell. Instead, he worked (before, during, and presumably after his work with the government on the instant contract) for a bank involved in potentially financing the federal work Mississippi Valley's sought to secure.[38] Therefore, Mr. Wenzel stood to financially gain if Mississippi Valley received the contract.

The government discovered the conflict after contract formation and voided the contract. Mississippi Valley then sued for breach damages and won at the Court of Claims.[39] The government petitioned for and was granted certiorari.[40] At the Supreme Court, the government argued Mr. Wenzell's conflict of interest gave the government cause to void the contract.[41]

The Supreme Court agreed. Mississippi Valley argued Mr. Wenzell was not an agent of the government because:

> [Mr. Wenzell] took no oath of office; he had no tenure; . . . he served without salary, except for $10 per day in lieu of subsistence; his duties were merely consultative, were occasional and temporary and were not prescribed by statute; and he was permitted to continue in his position as one of the vice presidents and directors of First Boston and to draw his salary from that company.[42]

---

[35] *See* Act of October 23, 1962, Pub. L. No. 87-849, 76 Stat. 1119, 1124-5.

[36] 364 U.S. 520 (1961).

[37] *Id.* at 525-47.

[38] *Id.*

[39] *See* Mississippi Valley Generating Co. v. United States, 147 Ct. Cl. 1 (1959).

[40] *See* United States v. Mississippi Valley Generating Co., 362 U.S. 939 (1960).

[41] *See* United States v. Mississippi Valley Generating Co., 364 U.S. at 524.

[42] *Id.* at 552 (quotations omitted).

The Supreme Court found Mr. Wenzell's employment not determinative.

> [Mr. Wenzell] who has taken no oath of office, who has no tenure, and who receives no salary is just as likely to subordinate the Government's interest to his own as is a regular, fulltime compensated civil servant. This is undoubtedly why [18 U.S.C. § 434] applies not only to those who are 'employed' by the Government, but also to '(w)hoever . . . acts' as an agent for the Government.[43]

Instead, the Supreme Court focused on the relationship between the parties, what the government knew and when it knew it, and Mr. Wenzell's contributions to the final deal. The Supreme Court's analysis turned on the extent of Mr. Wenzell's acquisition support services rather than formal titles or authority.[44]

Both *Mississippi Valley* and *Rankin* are great examples of how a generally applicable criminal law can guard against personally conflicted public procurement. What is especially noteworthy is how both cases arose in the context of a claim. Note that in *Strang*, the government acted in its sovereign prosecutorial role, using the law as a sword. In that case, the Supreme Court read the law, and particularly the bounds of agency, to be fairly limited. But when the government acted in its market role, using the law as a shield to defend against claims arising out of transactions rife with personal conflicts of interest, the courts read the generally applicable criminal law more generously. These cases demonstrate courts' ability to effectuate the proposed generally applicable criminal law's broader policy objectives without giving prosecutors expansive new powers.

B. Disharmonization: 1962–Present

In 1962, Congress created the current chapter 11 of title 18 to house the various criminal statutes regarding bribery, graft, and conflict of interest.[45] This rewrite replaced 18 U.S.C. § 434, and a host of other statutes, with the modern inception of the conflict of interest criminal statute, 18 U.S.C. § 208. 18 U.S.C. § 208 expanded the scope of potential criminal behavior from business transactions with a business the person held an interest in to any personal and substantial involvement with a particular matter touching upon the person's financial interests.[46] There was just one catch: 18 U.S.C. § 208 applied then, as it applies now, only to government employees. The coverage went from wide and thin to narrow and deep. The repeal of 18 U.S.C. § 434 without a replacement covering non-government employees decriminalized overnight what had been criminal for almost a hundred years.

---

[43] *Id.*

[44] *Id.* at 533 (describing the germane conduct).

[45] *See* Act of Oct. 23, 1962, Pub. L. No. 87-849, 76 Stat. 1119.

[46] *Compare* 18 U.S.C. § 208 (2013), *with* Act of June 25, 1948, ch. 645, § 434, 62 Stat. 683, 703 (germane law codified at 18 U.S.C. § 434).

Why the rewrite dropped coverage on those outside a federal employment status is not apparent from the Congressional Record.[47] The omission did not seem intentional. Congress was interested in ensuring the revised statutes, as a whole, facilitated recruitment of talent, especially temporary talent, to government service. In an effort to create a middle ground, Congress specifically created the "special government employee"[48] category to catch temporarily employed persons within 18 U.S.C. § 208 and other statutes.[49] This definition included those who worked for the government for fewer than 130 out of the preceding 365 days.[50] Such a category likely applied to the Mr. Wenzells of the 1960s. But it certainly has little value today. Rare is the one who (intentionally) works for the government fewer than 130 days out of the preceding 365 days. So why the enacted statutory scheme decriminalized contractor and grantee employees engaging in conflicted public acquisition is unknown.

With the disharmonization, conflict of interest law largely fractured into three separate bodies.[51] Each body of law will be examined to continue the story from 1962 to the present.

1. Government Employees

Developments in conflict of interest law after 1962 focused almost exclusively on federal employees. Initially, President John F. Kennedy issued an executive order that required various top level officials, board and commission members, and his staff to ensure their conduct did not result or appear to result in the "[u]se of public office for private gain[, a]ny loss of complete independence or impartiality[, or a]ny adverse effect on the confidence of the public in the integrity of the Government."[52] In 1965, President Lyndon B. Johnson further refined those rules, expanding their reach to any executive branch "employee" and spelling out specific prohibitions.[53] The Ethics in Government Act of 1978[54] codified the practice of routine financial disclosures for certain high level government employees[55] and established the

[47] *See, e.g.,* 107 Cong. Rec. H14,774-82 (Aug. 7, 1961), 108 Cong. Rec. S11,258-61 (June 21, 1962), 108 Cong. Rec. S21,975-92 (Oct. 3, 1962), 108 Cong. Rec. H22,311-3 (Oct. 4, 1962) (various debates and reports about the proposed and enacted law).

[48] *See* Act of October 23, 1962, Pub. L. No. 87-849, § 202, 76 Stat. 1119, 1121.

[49] *See* 18 U.S.C. § 202(a) (2013).

[50] Pub. L. No. 87-849, § 202, 76 Stat. 1121. The germane parts of the definition remain in the law today. *See* 18 U.S.C. § 202(a).

[51] Note that employees of parties in other transaction agreements (OTAs), like OTAs themselves, defy classification. As such, they will not be discussed particularly.

[52] Exec. Order No. 10,939, 26 Fed. Reg. 3,951 (May 6, 1961).

[53] *See* Exec. Order No. 11,222, 30 Fed. Reg. 6,469 (May 11, 1965). The order specifics were set against the same policy outlined in President Kennedy's order. *Compare id.* at § 201(c), *with* Exec. Order No. 10,939 at ¶ 2 (essentially the same six principals).

[54] Pub. L. No. 95-521, 92 Stat. 1824 (1978).

[55] *Id.* at Titles I, II, and III.

Office of Government Ethics (OGE).[56] Once the OGE became a separate agency in 1988,[57] President George H. W. Bush tasked the OGE with promulgating "a single, comprehensive, and clear set of executive-branch standards of conduct . . . ."[58]

In executing President Bush's order, the OGE built upon prior executive orders concerning ethics. For example, OGE prohibited federal employees from engaging "in a financial transaction using non-public information, nor allow the improper use of non-public information to further his own private interest or that of another, whether through advice or recommendation, or by knowing unauthorized disclosure."[59] This prohibition can be traced through prior executive orders. President Kennedy's 1961 order prohibited the few government employees it concerned from using "public office for private gain . . . ."[60] President Johnson's 1965 order expanded the application of the principle to all government employees and fleshed out its scope by explicitly prohibiting government employees from engaging "directly or indirectly, [in] financial transactions as a result of, or primarily relying upon, information obtained through their employment."[61] And President Bush's order refined that language to state "[e]mployees shall not engage in financial transactions using non-public Government information or allow the improper use of such information to further any private interest."[62]

---

[56] *Id.* at Title IV. Initially, the OGE was under the prior incarnation of the Office of Management and Budget. *See id.* at § 401(a) ("There is established in the Office of Personnel Management an office to be known as the Office of Government Ethics."). Later the OGE became a separate agency as it is today. Once a separate agency, the OGE became the regulatory authority for executive branch ethics programs and rule-making. *See Mission & Responsibilities*,United States Office of Government Ethics, http://www.oge.gov/About/Mission-and-Responsibilities/Mission---Responsibilities/ (last visited August 14, 2014).

[57] *See* Pub. L. No. 100-598, § 3, 102 Stat. 3031, 3031 (Nov. 3, 1988) (reauthorizing the Office of Government Ethics).

[58] *See* Exec. Order No. 12,674, § 201(a), 54 Fed. Reg. 15,159 (Apr. 12, 1989). Note President Bush later modified this executive order; however, the modifications are not germane to this article. *Compare* Exec. Order No. 12,731, 55 Fed. Reg. 42,547 (Oct. 17, 1990), *with* Exec. Order No. 12,674, 54 Fed. Reg. 15,159 (Apr. 12, 1989) (minor changes to appointees and delegations).

[59] Standards of Ethical Conduct for Employees of the Executive Branch, 5 C.F.R. § 2635.703(a) (2013) (use of non-public information). *See also* Standards of Ethical Conduct for Employees of the Executive Branch, 57 Fed. Reg. 35,006, 35,032 (Aug. 7, 1992) (this rule's "broad reach is a consequence of the breadth of the underlying principle as stated in [Executive Order 12,674]. While specifically prohibiting an employee from engaging in a 'financial transaction' using non-public information, the principle provides further that an employee shall not allow the use of non-public information to further 'any private interest.' The purpose of the principle is as much to protect non-public information as it is to ensure that the employee and others do not profit from the improper disclosure of such information.").

[60] Exec. Order No. 10,939, § 2(a), 26 Fed. Reg. 3,951, 3,951 (May 6, 1961).

[61] Exec. Order No. 11,222, § 203(b), 30 Fed. Reg. 6,469, 6470 (May 11, 1965).

[62] Exec. Order No. 12,731, § 101(c), 55 Fed. Reg. 42,547, 42, 547 (Oct. 17, 1990).

And that is where we are today: 18 U.S.C. § 208 and various interpretative regulations.[63]

2. Contractor Employees

After 1962, contractor employees' conflicts of interest were controlled, if at all, by *ad hoc* means. Some agencies passed regulations.[64] Some mandated contract clauses.[65] Others negotiated clauses particular to certain contracts.[66] Without a generally applicable criminal law, the gaping hole left in 1962 became more and more pronounced during the extensive outsourcing of governmental functions, to include acquisition functions, during the first decade of the twenty-first century.

In 2007, the Acquisition Advisory Panel[67] ("Panel") gave some attention to the disharmonization in ethics controls between government and contractor employees who were executing similar work but operating under entirely different ethics regimes.[68] While the Panel ultimately "concluded that it was not necessary to adopt any new federal statutes to impose additional [conflict of interest] requirements upon contractors or their personnel,"[69] the Panel did recommend the FAR Council review the current regime and "create new, uniform, government-wide policy and clauses dealing with . . . personal conflicts of interest, as well as the protection of contractor confidential and proprietary data."[70]

---

[63] *See infra* Figure 1.

[64] *See infra* Figure 2.

[65] *See id.*

[66] *See* U.S. Gov't Accountability Office, GAO-08-169, Defense Contracting: Additional Personal Conflict of interest Safeguards Needed for Certain DoD Contractor Employees 52-6 (2008), *available at* http://www.gao.gov/new.items/d08169.pdf (discussing selected conflict of interest clauses).

[67] The Panel was created to "to review laws and regulations regarding the use of commercial practices, performance-based contracting, the performance of acquisition functions across agency lines of responsibility, and the use of Governmentwide contracts." National Defense Authorization Act for Fiscal Year 2004, Pub. L. No. 108-136, § 1423(a), 117 Stat 1392, 1663 (Nov. 24, 2003). While the Panel was not specifically tasked to review the development of the blended workforce, the Panel found addressing the matter "essential . . . ." Acquisition Advisory Panel, Report Of the Acquisition Advisory Panel to the Office of Federal Procurement Policy and the United States Congress 23 (2007), *available at* https://www.acquisition.gov/comp/aap/24102_GSA.pdf.

[68] *See* Acquisition Advisory Panel, *supra* note 67.

[69] *Id*. at 423.

[70] *Id.* at 25 (parentheticals omitted). *See also Id.* at 389-419 (chapter entitled "Appropriate Role of Contractors Supporting Government"); *Id.* at 407-13 (discussing "Personal Conflicts of Interest" for contractor employees); *Id.* at 422-6 (discussing related recommendations).

Some in Congress took this part of the Panel's recommendations to heart. In the Senate, the Accountability in Government Contracting Act of 2007 ("AGCA") was introduced.[71] A similar bill was introduced in the House.[72] Both versions essentially sought to study the issue further. Both passed their respective chambers but not the other chamber. And neither bill had anything to do with grantee employees.

The issue remained alive outside of Congress.[73] In March 2008, the FAR Council opened a case requesting comments on "if, when, and how service contractor employees' [personal conflict of interest] need to be addressed . . . ."[74] The FAR Council extended the comment period once[75] and received 14 comments.[76] The comments ranged from supporting the general thrust of the regulation to stating the current decentralized agency-specific regime was sufficient.[77]

While the FAR Council pondered the matter, Congress moved up their timeline through section 841 of the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 (hereinafter "Section 841").[78] Section 841 required the Administrator for Federal Procurement Policy to "develop and issue a standard policy to prevent personal conflicts of interest by contractor employees performing acquisition functions closely associated with inherently governmental functions . . . ."[79] The FAR Council opened a new FAR case[80] and, after notice

---

[71] *See* Accountability in Government Contracting Act of 2007, S. 680, 110th Cong. § 209(b) (as passed by Senate, Nov. 7, 2007).

[72] *See* Accountability in Contracting Act, H.R. 1362, 110th Cong., § 302(a) (as passed by House, Mar. 15, 2008).

[73] *See, e.g.,*U.S. Gov't Accountability Office, *supra* note 66; E-mail from ContactOGE@oge.gov, to author (Sept. 27, 2012, 08:41 EST) (on file with author) (containing June 2007 speech from OGE Director Robert I. Cusick to the Defense Industry Initiative on Business Ethics and Conduct).

[74] *See* Federal Acquisition Regulation, Service Contractor Employee Personal Conflicts of Interest, 73 Fed. Reg. 15,961, 15,961 (Mar. 26, 2008) (comments requested) [hereinafter FAR].

[75] *See* FAR, Service Contractor Employee Personal Conflicts of Interest, 73 Fed. Reg. 34,600 (June 17, 2008) (comment period extended).

[76] *See* FAR, Service Contractor Employee Personal Conflicts of Interest (June 4, 2008), *available at* http://www.regulations.gov/#!documentDetail;D=FAR-FAR-2008-0002-0025.

[77] *See id.*

[78] *See* Duncan Hunter National Defense Authorization Act for Fiscal Year 2009, Pub. L. No. 110-417, § 841, 122 Stat. 4,356, 4,537-9 (Oct 14, 2008) (codified in 41 U.S.C. § 2303 (2013)).

[79] *Id.* at § 841(a).

[80] *See* FAR, Preventing Personal Conflicts of Interest for Contractor Employees Performing Acquisition Functions, 74 Fed. Reg. 58,584-9 (Nov. 13, 2009) (FAR Case 2008-025). The prior FAR case, FAR Case 2007-017, was withdrawn on June 29, 2010, a date between the first issuance of FAR Case 2008-025 on November 13, 2009, and the resulting final rule publication on November 2, 2011. *See* RIN Data, RIN: 9000-AK97, FAR, Service Contractor Employee Personal Conflicts of Interest (2012), *available at* http://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201104&RIN=9000-AK97. The Federal Register for June 29, 2010, does not contain a reference to the withdrawing of FAR Case 2007-017. *See* Recovery Accountability and Transparency Board, 75 Fed. Reg. 37,287-706 (June 29, 2010).

and comment,[81] published what is now known as FAR Subpart 3.11 in November of 2011.[82]

And that is where we are today: FAR Subpart 3.11 overlaying a patchwork of (mostly) regulations and contract clauses.[83]

3. Grantee Employees

Chapter 11 of title 18 and implementing and supplemental regulations establish the norms for government employees confronted with conflicts of interest. FAR Subpart 3.11, in a fashion, functions similarly for contractor employees. But little similar general guidance exists within the grant community.

The only generally applicable conflict of interest control is found in Office of Management and Budget (OMB) guidance and forms.[84] OMB initially received authority to "prescribe such rules and regulations as are deemed appropriate" for grant administration in 1968 under the Intergovernmental Cooperation Act of 1968.[85] OMB has retained that authority over time.[86] OMB has issued various circulars, beginning in 1971, to provide guidance on grant award and administration, to standards of conduct regarding conflicts of interest.[87]

While the conflict of interest rules for grantee employees are much less defined, courts have affirmed the government's ability to void a grant award tainted with conflict of interest as was done in *Mississippi Valley.* In *Town of Fallsburg v.*

---

[81] *See* FAR, Preventing Personal Conflicts of Interest for Contractor Employees Performing Acquisition Functions (June 4, 2008), *available at* http://www.regulations.gov/#!documentDetail;D=FAR-2009-0039-0018.

[82] *See* FAR, Preventing Personal Conflicts of Interest for Contractor Employees Performing Acquisition Functions, 76 Fed. Reg. 68,017 (Nov. 2, 2011).

[83] *See infra* Figure 2.

[84] *See infra* Figure 3.

[85] Pub. L. No. 90-577, § 403, 82 Stat. 1098, 1104 (Oct. 16, 1968).

[86] This area of the code has seen significant revision. *See, e.g.,* Chief Financial Officers Act of 1990, Pub. L. No. 101-576, § 202, 104 Stat. 2838, 2840 (Nov. 15, 1990); Pub. L. No. 97-258, §§ 6301-8, 96 Stat. 877, 1003-5 (Sept. 13, 1982). However, through those revisions and through today, OMB retained authority to set general grant award and administration policy. *See* 31 U.S.C. § 503(b)(2)(C) (2013) (currently, the OMB Deputy Director for Management is so tasked).

[87] *See* Grants and Cooperative Agreements with State and Local Governments, 59 Fed. Reg. 52,224, 52,225 (Oct. 14, 1994) (requiring agencies to use the SF-424c and SF-424d for applications); Grants and Cooperative Agreements with State and Local Governments, 53 Fed. Reg. 8,028, 8,030 (Mar. 11, 1988) (same). *See also* Uniform Administrative Requirements for Grant and Agreements with Institutions of Higher Education, Hospitals and Other Non-profit Organizations, 58 Fed. Reg. 62,992, 63,001 (Nov. 29, 1993) (stating the same conflict of interest prohibition currently stated at 2 C.F.R. § 215.42); Uniform Administrative Requirements for Grants and Agreements With Institutions of Higher Education, Hospitals, and Other Non-Profit Organizations (OMB Circular A-110), 69 Fed. Reg. 26,281 (May 11, 2004) (moving OMB Circular No. A-110 to the Code of Federal Regulations).

*United States*,[88] the EPA withheld cost-sharing Clean Water Act grant funds from the Town of Fallsburg, New York, when the Town Supervisor responsible for awarding the grant-funded contracts, had a conflict of interest. The U.S. Attorney charged and convicted the Town Supervisor of mail fraud, false statements, racketeering, and other offenses involving the conflicted grant-funded contracts. The district court specifically found that the Town Supervisor had not fully disclosed his financial relationship with awardee contractor, had not refrained from contract administration duties as directed, and had executed various forms fraudulently to cover his conflict.[89]

The grant administrator pulled funding pursuant to the grant's terms finding that the grantee, the Town of Fallsburg, had failed to comply with the "Grantee Responsibility for Standards of Conduct."[90] On appeal, the court utilized an Administrative Procedures Act (APA) standard of review[91] and held the agency's decision reasonable thus affirming a modern-day version of *Mississippi Valley*.

And that is where we are today: various mandatory OMB regulations and standard forms and a helpful case.[92]

## III. A GENERALLY APPLICABLE CRIMINAL LAW WOULD ADDRESS THE INADEQUACIES OF THE CURRENT PATCHWORK

This part examines how contractual and regulatory solutions are inadequate and why a generally applicable criminal law is necessary. The vacuum Congress left in 1962 invited, nay mandated, contractual and regulatory solutions from agencies most affected. But without a generally applicable criminal law on which to build, these efforts were spotty, narrow, and redundant. As Figures 2 and 3 demonstrate, contractual or regulatory solutions come in all shapes and sizes. Without a common foundation, harmonization is difficult, unnecessary, and unvalued. Agency-developed mechanisms share limited application, dissimilar means, and cannot hold individuals responsible. A generally applicable criminal law would create the structure on which to address those shortcomings. A generally applicable criminal law would create the necessary foundation. And that foundation, agencies could implement nuanced control mechanism, learn from others' experiences, and rely on the criminal justice system for incredibly bad cases. One need only look at the entire ethics regime crafted around 18 U.S.C. § 208 to see how a single criminal law can support a vibrant house of anti-corruption controls. A similar law applicable to contractor and grantee employees could do the same.

---

[88] Town of Fallsburg v. United States, 22 Cl. Ct. 633 (1991).

[89] *Id.* at 638-9.

[90] *Id.* at 639-40.

[91] *Id.* at 641-2.

[92] *See infra* Figure 3.

A. Concerning Contractors, Why the Current Patchwork is Inadequate

Effective December 2, 2011,[93] FAR Subpart 3.11 was the first real macro-level attempt at controlling conflicts of interest amongst contractor employees engaged in public acquisition. Prior regulations concerned organizational conflicts of interest,[94] though such regulations need not have been so limited.[95] FAR Subpart 3.11 perhaps attempted to create a common foundation on which agency FAR supplements could build. However, it too suffers from limitations of application, purpose, and reach.

The analysis below will detail many of FAR Subpart 3.11's core problematic issues. Special attention will be paid to how particular issues evince a need for a generally applicable criminal law rather than administrative tinkering.[96]

1. It Doesn't Require What it's Supposed to Require

Congress mandated FAR regulations that would prevent personal conflicts of interest by contractor employees performing acquisition support functions.[97] What Congress got were FAR regulations that mandated contractors establish a system reasonably calculated to prevent employees from performing acquisition support services while conflicted. Thus, Congress got a system geared toward a result rather than the result itself. This switch is especially evident when comparing

---

[93] FAR, Preventing Personal Conflicts of Interest for Contractor Employees Performing Acquisition Functions, 76 Fed. Reg. 68,017, 68,026 (Nov. 2, 2011).

[94] *See* Federal Acquisition Regulations for National Aeronautics and Space Administration, 48 C.F.R. subpart 9.5 (2013) [hereinafter FAR].

[95] *See* National Defense Authorization Act for Fiscal Year 1989, Pub. L. No. 100-463, § 8141, 102 Stat. 2270, 47-8 (Oct. 1, 1988) (requiring the enactment of regulations concerning conflict of interest standards for "persons" providing "such . . . services related to Federal contracts . . . to the extent necessary to identify and evaluate the potential for conflicts of interest that could be prejudicial to the interests of the United States.") (codified at 41 U.S.C. § 2304). *See also* 41 U.S.C. § 1121(a),(b) (2013) (the Administrator of the Office of Federal Procurement Policy "shall provide overall direction of procurement policy and leadership in the development of procurement systems [and] may prescribe Government-wide procurement policies.").

[96] *See, e.g.,* National Defense Authorization Act for Fiscal Year 2013, Pub. L. No. 112-239, § 829, 126 Stat. 1632, 1841-2 (Jan. 2, 2013) (directing the Secretary of Defense to "review the guidance on personal conflicts of interest for contractor employees . . . in order to determine whether it would be in the best interest of the Department of Defense and the taxpayers to extend such guidance" beyond contractor employees providing acquisition support services); Review of Regulatory Coverage Regarding Prevention of Personal Conflicts of Interest for Contractor Employees, 76 Fed. Reg. 68,046 (Nov. 2, 2011) (requesting public comment on whether FAR Subpart 3.11 should be expanded in coverage or application on the same day FAR Subpart 3.11 was promulgated).

[97] Duncan Hunter National Defense Authorization Act for Fiscal Year 2009, Pub. L. No. 110-417, § 841(a), 122 Stat. 4356, 4537-9 (2008). The law particularly applies to contractors whose contracts "involve performance of acquisition functions closely associated with inherently governmental functions for, or on behalf of, a Federal agency or department." *Id.* at § 841(a). *See also* FAR, 48 C.F.R. 3.1106(a)(2) (2013).

the statutory basis for the two thrusts of FAR Subpart 3.11: conflicts of interest and use of non-public information.

Congress's policy directive and listing of policy elements concerned conflicts of interest. Congress first mandated "develop[ment] and issu[ance of] a standard policy to prevent personal conflicts of interest by contractor employees performing acquisition [support] functions . . . ."[98] Congress then, as one of seven policy enumerated elements, stated the developed policy shall require contractors to "identify and prevent" personal conflicts of interest.[99] Thus, Congress set a policy floor in the listing of elements (i.e., contractors must have a system) and set a policy objective in the directive (i.e., prevent contractor employees' personal conflicts of interests).

In comparison, Congress only set a policy floor for controlling use of non-public information, namely that "each contractor whose employees perform [acquisition support services must] . . . prohibit contractor employees who have access to non-public government information obtained while performing such [acquisition support services] from using such information for personal gain . . . ."[100] Controls on use of non-public information do not appear in the earlier policy directive.[101]

Therefore, crafting FAR Subpart 3.11 to require contractors adopt certain internal employment policies and ensure employees accomplish non-disclosure agreements satisfies only statutory policy elements. However, crafting FAR Subpart 3.11 to not actually mandate the prevention of "personal conflicts of interest by contractor employees performing" acquisition functions fails to meet the larger policy directive.

The distinction has a difference. In doing so, the regulation shifted the ultimate compliance burden from the contractor to the contractor's employee.[102] The comments to the final rule explicitly stated how the rule intentionally shifted the burden off the contractor: "There is nothing in the [implementing] clause that establishes contractor liability for a violation by an employee, as long as the con-

---

[98] Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 § 841(a).

[99] *Id.* at § 841(a)(1)(B)(i).

[100] *Id.* at § 841(a)(1)(B)(ii).

[101] *Id.* at § 841(a).

[102] For example of a contractor counsel noting and using this burden shifting to the contractor's advantage, see Keith R. Szeliga & Franklin C. Turner, *Preventing Personal Conflicts of Interest Among Contractor Employees Performing Acquisition Support Services*, 12-4 Briefing Papers 1, 6 (2012) ("Although [it] is unlikely that covered employees will seek or obtain financial disclosures from [other members of the household] in all cases, informing them of the obligation to do so will protect the contractor's interests."). *See also* Professional Services Council, Review of Regulatory Coverage Regarding Prevention of Personal Conflicts of Interest for Contractor Employees (FAR PCI Comment) at 2, *available at* http://www.regulations.gov/#!documentDetail;D=FAR-2011-0091-0002 (government services trade association similarly recognizing the burden shifting).

tractor followed the appropriate steps to uncover and report the violation."[103] The difference is subtle yet important, especially in the civil False Claims Act context.[104]

Revising the regulation to shift ultimate compliance back to the contractor would help meet the explicit Congressional policy directive. If a contractor was liable "for a violation by an employee,"[105] the government would have its traditional contract breach remedies and, potentially, a civil False Claims Act case. But doing so may be impossible because the FAR, through its implementing clauses, binds contractors, not their employees. Save a sole proprietorship contractor, the government is only in privity with the contractor rather than the individual employees. Thus, even if the regulation shifted ultimate compliance back to the contractor, creating essentially a strict liability compliance pitfall, the regulation could not do what 18 U.S.C. § 434 could have done: hold the individual responsible and clearly support any subsequent contract voiding or termination for an acquisition support contractor employee's conflict of interest.

2. No Effective Oversight or Compliance Mechanisms

President Ronald Reagan was famously fond of the Russian maxim *dovorey no provorey*, meaning "trust, but verify."[106] Unfortunately, FAR Subpart 3.11 makes the government trust the contractor with few means of verification. The regulation provides no mechanism to verify whether the responsive systems actually identify and prevent personal conflicts of interest and prohibit the use of non-public information for personal gain. The regulation does not facially provide the contracting officer access to the non-disclosure agreements or financial interest disclosures.[107] In fact, the regulation directs suspicious contracting officers to "contact the agency legal counsel for advice . . . ."[108] While the communication with one's legal counsel could be beneficial, open communication between the contracting officer and the contractor could likely be more beneficial. Clear authority for routine records access

---

[103] FAR, Preventing Personal Conflicts of Interest for Contractor Employees Performing Acquisition Functions, 76 Fed. Reg. 68,017, 68,022 (Nov. 2, 2011).

[104] *See* United States v. Sci. Applications Int'l Corp., 626 F.3d 1257 (D.C. Cir. 2010) (holding a contractor with organizational conflicts of interest who submits vouchers for payment of advisory services can be civilly liable under the False Claims Act when conflict-free advisory services were material to the government's decision to pay); United States ex rel. Harrison v. Westinghouse Savannah River Co., 176 F.3d 776 (4th Cir. 1999) (similarly holding an organizational conflict of interest can substantiate a False Claims Act case).

[105] Preventing Personal Conflicts of Interest for Contractor Employees Performing Acquisition Functions, 76 Fed. Reg. at 68,022.

[106] Ronald Reagan, Remarks on Signing the Intermediate-Range Nuclear Forces Treaty (Dec. 8, 1987), *available at* www.reagan.utexas.edu/archives/speeches/1987/120887c.htm.

[107] *See* FAR, 48 C.F.R. 3.1103(a)(1) (2013) (contractor manages entire process).

[108] *See* FAR, 48 C.F.R. 3.1105 (2013) (contracting officers who suspect "violation[s] by the contractor . . . shall contact the agency legal counsel for advice . . . .").

could drive early and open communications, reducing compliance and potential litigation costs.

Many current mechanisms for potentially accessing the information are insufficient. Under the standard services inspection clauses, the government may review the "[c]omplete records of all inspection work . . . ."[109] As the provision of acquisition support services free of conflicts of interests is not a contract requirement (only the creation and maintenance of a preventative system is), inspection records would not necessarily include an individual's financial disclosure.[110] More likely, responsive inspection records would only indicate an individual completed a financial disclosure and the contractor found no conflict of interest. Similarly, quality assurance surveillance may be similarly ineffectual. Contract administrators cannot readily observe and measure personal conflicts of interest in the work place.[111] Also, the audit clause applies to records substantiating costs rather than quality.[112] Finally, disclosures under the business ethics rule may be untimely for an on-going acquisition.[113]

While the regulations leave the government fairly blind, if the government were to discover a contractor employee's conflict of interest, the regulation gives little further guidance. The draft regulation listed five remedies,[114] though that language was later removed as unnecessarily duplicative.[115] While the listed remedies

[109] FAR, 48 C.F.R. 52.246-4(b) (2013); FAR, 48 C.F.R. 52.246-5(b) (2013).

[110] Potentially, a savvy contracting officer could add language to the performance work statement stating that acquisition support services shall be performed "by persons free of conflicts of interest." However, this then begs the question why not state such services also be "good," "timely," "accurate," "insightful," or any other descriptor one would hope would go without saying.

[111] *See* FAR, 48 C.F.R. 46.401(a) (2013) (quality assurance occurs to "determine that . . . services conform to contract requirements.").

[112] *See* FAR, 48 C.F.R. 52.215-2(b) (2013). The promulgating clause expands the access to "records . . . to satisfy contract negotiation, administration, and audit requirements . . . ." FAR, 48 C.F.R. 4.703(a) (2013). However, the clause grants access only for cost records. *See* FAR 52.215-2(b) (2013); FAR, 48 C.F.R. 52.215-2(c) (records supporting a contractor's certified cost or pricing data); FAR, 48 C.F.R. 52.215-2(d) ("directly pertinent records" the Government Accountability Office requests); FAR, 48 C.F.R. 52.215-2(e) (materials supporting contractor prepared reports). *See also* FAR, 48 C.F.R. 52.214-26 (2013) (similar language for contracts procured with sealed bidding procedures).

[113] *See* FAR, 48 C.F.R. 52.203-13(c)(2)(ii)(G) (2013). A contractor would report delivery of conflicted acquisition support services as a potential civil False Claim violation. *See* United States v. Sci. Applications Int'l Corp., 626 F.3d 1257 (D.C. Cir. 2010) (holding a contractor with organizational conflicts of interest who submits vouchers for payment of advisory services can be civilly liable under the False Claims Act when conflict-free advisory services were material to the government's decision to pay).

[114] *See* Preventing Personal Conflicts of Interest for Contractor Employees Performing Acquisition Functions, 74 Fed. Reg. 58,584, 58,589 (Nov. 13, 2009) (proposed FAR, 48 C.F.R. 52.203-16(d)).

[115] *See* Preventing Personal Conflicts of Interest for Contractor Employees Performing Acquisition Functions, 76 Fed. Reg. 68,017, 68,022 (Nov. 2, 2011) ("While the list of remedies included within FAR 52.203-16 specifically identified those remedies available for violations involving potential conflicts, it was not intended to create new remedies. For this reason, the Councils have removed

gave the government no new authority, their inclusion would have clarified their applicability and put the contractor that much more on notice.

Beyond restating or reaffirming what already is, the regulation did not provide a new remedy. The remedies previously listed[116] have limited applicability especially for medium to small sized violations. In such violations (and large ones too), a procurement may need to be redone,[117] or a resulting contract voided or terminated,[118] thus generating significant reprocurement and/or termination costs.[119] A violation could also trigger civil penalties under the False Claims Act.[120] While the law does allow the government to recover such costs, stating that remedy clearly, along with other ones, would have better communicated to all what remedies are available.

Additionally, FAR Subpart 3.11 has no remedy against an individual. Thus, enforcement is limited to actions the contractor takes against the employee. While the most powerful of these actions, firing, is certainly a motivator, the regulation does not, and could not, require that occurrence. The most the regulation could do is empower the contracting officer to prohibit the contractor from assigning that employee to the acquisition support function of the contract. That employee could still work for the contractor on a different part of the contract or in a different business segment.

Potentially, the agency could suspend or debar an individual.[121] A suspended or debarred individual would be "excluded from conducting business with the

---

the paragraph . . . .").

[116] Those remedies were suspension of contract payments, loss of award fee, termination for default, disqualification from subsequent related contractual efforts, and suspension or debarment. *See* Preventing Personal Conflicts of Interest for Contractor Employees Performing Acquisition Functions, 74 Fed. Reg. 58,584, 58,589 (Nov. 13, 2009) (proposed FAR, 48 C.F.R. 52.203-16(d)).

[117] While typically, the case law speaks in terms of conflicts of interest by government employees, *see, e.g.,* Savannah River Alliance, B-311126, 2008 CPD ¶ 88 (Comp. Gen. Apr. 25, 2008) (protestor alleged federal employee who gave references checks of key personnel had a personal conflict of interest when she gave a positive reference check to an offeror who employed her husband and a negative reference check to the protestor), it takes little imagination to envision a contractor employee doing action that lead to the protest. *See, e.g.,* Celadon Laboratories, Inc., B-298533, 2006 CPD ¶ 158 (Comp. Gen. Nov. 1, 2006) (protestor alleged personal conflicts of interest on the part of non-government technical evaluators for a Small Business Innovation Research program phase I selection).

[118] *See* PGBA, L.L.C. v. United States, 389 F.3d 1219 (Fed. Cir. 2004) (affirming Court of Federal Claims decision to exercise discretion in whether to set aside an awarded contract despite material errors in the award process and decision).

[119] *See* CDA, Inc. v. Soc. Sec. Admin., CBCA 1558, 12-1 BCA ¶ 34,990 (Mar. 28, 2012) (stating the three elements necessary for the government to recover reprocurement costs).

[120] *See* United States v. Sci. Applications Int'l Corp., 626 F.3d 1257 (D.C. Cir. 2010) (holding a contractor with organizational conflicts of interest who submits vouchers for payment of advisory services can be civilly liable under the False Claims Act when conflict-free advisory services were material to the government's decision to pay).

[121] *See* FAR, 48 C.F.R. 9.406-2(c) (2013) (allowing debarment "based on any other cause of

Government as agents or representatives of other contractors."[122] However, the contractor employer could still employ that person in a different business segment. Therefore, the government has little motivation to pursue suspension and debarment of individuals as the listing's effect is comparable to what the contracting officer can do under FAR Subpart 3.11.

Simply adding language affirmatively providing the contracting officer, or his designee, access to FAR 52.203-16 generated documents would address the records issue.[123] However, the other identified and recurring issue would remain.

A criminal law would provide contractors significantly more motivation to prevent conflicts and cooperate with investigations. And a criminal law would give the government recourse against an individual and potentially the contractor, under egregious enough facts, for aiding and abetting, conspiracy, or under other criminal liability theories.

3. Commercial Items Exemption

Federal Acquisition Regulation Subpart 3.11 completely exempted commercial procurements.[124] The FAR Council hitched this change to the comments.[125] However, no submitted comment suggested such an exemption.[126] The commercial items exemption did not appear in the draft rule.[127] The exemption first appeared in the final rule.

---

so serious or compelling a nature that it affects the present responsibility of the contractor or subcontractor."); FAR, 48 C.F.R. 9.407-2(c) (2013) (allowing suspension "for any other cause of so serious or compelling a nature that it affects the present responsibility of a Government contractor or subcontractor.").

[122] FAR, 48 C.F.R. 9.405(a) (2013).

[123] *See generally* FAR, 48 C.F.R. 3.502-2(h) (2013); FAR, 48 C.F.R. 52.203-7(c)(3) (2013) (implementation of the Anti-Kickback statute that allows government inspection of relevant contractor records when a violation is suspected).

[124] *See* Preventing Personal Conflicts of Interest for Contractor Employees Performing Acquisition Functions, 76 Fed. Reg. 68,017, 68,025 (Nov. 2, 2011) (proposed FAR, 48 C.F.R. 3.1106 and amended FAR, 48 C.F.R. 12.503(a) (2013) containing an exemption for commercial items and services).

[125] *See id.* at 68,017 (stating the Council reviewed the comments and "[a]s a result of this review, the Councils have incorporated some changes in the final rule, including the following more significant changes . . . [a]mended 12.503(a) to clarify that the statute [41 U.S.C. § 2303 (2013)] does not apply to contracts for the acquisition of commercial items."). *See* 41 U.S.C. § 2303 (2013). This statute is a January 4, 2011, codification of Section 841. The statute says nothing about commercial items.

[126] *See* FAR, Preventing Personal Conflicts of Interest for Contractor Employees Performing Acquisition Functions, *available at* http://www.regulations.gov/#!documentDetail;D=FAR-2009-0039-0018 (Jan. 13, 2010) (Transmittal Memo and Comments # 1-19).

[127] *See* Preventing Personal Conflicts of Interest for Contractor Employees Performing Acquisition Functions, 74 Fed. Reg. 58,584, 58,584-9 (Nov. 13, 2009) (not including an exclusion of applicability for commercial item procurements).

This exemption appears to be more a result of inaction rather than action. Both Section 841 and FAR Subpart 3.11 were enacted after October 14, 1994. Section 841 did not contain any criminal or civil penalties or a specific statement of applicability to commercial procurements, nor did the FAR Council make a written determination to make Section 841 applicable to commercial item procurements. Thus, Section 841 and the resulting FAR Subpart 3.11 are not applicable to commercial procurements.[128] Presumably, Congress knew the language "any contract"[129] without more really meant "any noncommercial contract." But, it is possible they simply forgot and no one told them.

It is perhaps more unfortunate the potential Congressional oversight became an actual oversight when the FAR Council published the draft FAR Subpart 3.11 without the commercial items exemption. Potentially, some public comment could have been received on the issue. Such comments would not have been in vain as the FAR Council had authority then, as it does now, to apply Section 841, and thus FAR Subpart 3.11, to commercial purchases.

It is also possible this oversight caused certain commenters to approve of the draft rule. For example, the Inspector General (IG) of the General Services Administration (GSA) submitted a public comment to the predecessor FAR Case, FAR Case 2007-017, supporting "the development of a [FAR] Rule that addresses the issue of personal conflicts of interest among service contractor employees."[130] While the comment does not specifically state the IG hopes the GSA would benefit from such a rule, one can fairly assume the busy IG lent his support in hopes of having such a rule apply to at least part of his oversight portfolio. When FAR Council published the draft rule, with the commercial items exemption omitted, the Director, Internal Evaluation and Analysis, GSA IG, submitted extensive substantive suggestions and recommendations, stating the office of the GSA IG "strongly supports the intent of the [draft rule]."[131] Presumably, the IG and his office "strongly support[ed]" the draft rule and spent resource trying to improve it because they thought it would apply

---

[128] Procurement laws passed after October 13, 1994, are inapplicable to commercial procurements unless the FAR Council "makes a written determination that it would not be in the best interest of the Federal Government to exempt contracts for the procurement of commercial items from the applicability of the [law]." *See* 41 U.S.C. § 1906(b)(2) (2013); the law "provides for criminal or civil penalties." *Id.* at (d)(1); or, the law expressly states applicability to commercial item procurements. *Id.* at (d)(2).

[129] Duncan Hunter National Defense Authorization Act for Fiscal Year 2009, Pub. L. No. 110-417, § 841(a)(3)(A), 122 Stat. 4356, 4538 (Oct. 14, 2008) (Section 841(a) "shall apply to any contract for an amount in excess of the simplified acquisition threshold . . . .").

[130] *See* FAR, FAR Case 2007-017, Service Contractor Employee Personal Conflicts of Interest at 9 (June 4, 2008), *available at* http://www.regulations.gov/#!documentDetail;D=FAR-FAR-2008-0002-0025.

[131] *See* FAR, FAR Case 2008-025, Preventing Personal Conflicts of Interest for Contractor Employees Performing Acquisition Functions at 85 (Jan 13, 2010), *available at* http://www.regulations.gov/#!documentDetail;D=FAR-2009-0039-0018.

to a significant portion of their acquisition support services schedules.[132] Had the draft rule clearly communicated that commercial purchases, and thus a significant chunk of GSA facilitated transactions, would be inapplicable, the GSA IG might have had different input.

Understanding how, legally, this exemption came to pass is not the same as justifying it. Why is the provision of commercial acquisition support services less prone to conflict of interest risk than noncommercial acquisition of support services?[133] Why, for example, are commercial acquisition support services less prone to conflict of interest risk than noncommercial conflict of interest? Has anyone even asked the question? It is perhaps that last question that is the most unsettling as it is presently the most important of the three.

A generally applicable criminal law would clarify that Congress meant "any contract" when it said "any contract" in Section 841. Such a law would make clear Congress wanted the regulatory product of Section 841 applicable to commercial procurements. At a minimum, such a law would cause the FAR Council to revisit both the terms and applicability of FAR 3.11.

4. Untethered and Ambiguous Definitions

Many definitions in FAR Subpart 3.11 are awkward, unhelpful, vague, and ripe for litigation. A catalogue of them could be a paper in of itself.[134] As an example, this section will examined and demonstrate how one of the most important definitions is also amongst the most problematic.

Currently, a "personal conflict of interest" exists only when the competing interest "could impair the employee's ability to act impartially and in the best interest of the Government . . . ."[135] When "could" an interest so impair an employee? The FAR provides an "example" list of interests that "may" give raise to conflicting

---

[132] For examples of GSA schedules offering, in part, commercial acquisition support services, s*ee, e.g.,* GSA Federal Acquisition Service, Schedule 520, Financial and Business Solutions, HTTP://WWW.GSAELIBRARY.GSA.GOV/ELIBMAIN/SCHEDULESUMMARY.DO?SCHEDULENUMBER=520 (last visited Apr. 3, 2013); GSA Federal Acquisition Service, Schedule 871, Professional Engineering Services, http://www.gsaelibrary.gsa.gov/ElibMain/scheduleSummary.do?scheduleNumber=871(last visited Apr. 3, 2013); GSA Federal Acquisition Service, Schedule 874, Mission Orientated Business Integrated Solutions (MOBIS), http://www.gsaelibrary.gsa.gov/ElibMain/scheduleSummary.do?scheduleNumber=874 (last visited Apr. 3, 2013).

[133] In fact, one must wonder how acquisition support services can even be a commercial item. Federal acquisition is unique to the federal government. Perhaps this is an example of how the "of a type" language has been stretched too far. *See* FAR, 48 C.F.R. 2.101 (2013) (definition of commercial item).

[134] *See, e.g.,* David J. Ginsberg & Robert R. Bohn, *Let's Get Personal: A Guide to the Interpretation and Implementation of the FAR Personal Conflicts of Interest Rules*, 47-SUM PROCUREMENT LAW. 11, 13-6 (2012) (identifying various "Interpretation and Implementation Challenges").

[135] FAR, 48 C.F.R. 3.1101 (2013); FAR, 48 C.F.R. 52.203-16(a) (2013).

interests.[136] But the terms "example" and "may" affirm the possibility the listed interests might not always give rise to a conflicting interest.[137] For example, could a highly paid contractor employee's $1K equity investment in a $1M portfolio "impair" his performance of acquisition support services? What about a lowly paid contractor employee's $1K equity investment in a $5K portfolio?

The definition of a "personal conflict of interest" invites subjective analysis and the exercise of discretion. But the regulation vests the analysis and decision with the contractor, mandating involvement of the contracting officer only if an incident occurred.[138] Are contractors really the best situated to make those decisions? Do contractors really want to make those decisions—and risk the government, years later, second-guessing them? Will not quality fall over time as contractors with assertive and proactive compliance officers drive up costs for quality, and contractors with more liberal interpretations become more competitive in a more cost-driven acquisition system? Who will the market encourage as price continues to drive fiscally strapped agencies?

The purported safe harbor of "*de minimis*" is unhelpful.[139] The definition of *de minimis* is essentially the absence of a personal conflict of interest. Presumably, the FAR Councils wanted to carve out a grey zone between a personal conflict of interest and no personal conflict of interest, much like the Office of Government Ethics has for federal employees.[140] However, in their unwillingness to do the necessary spade work,[141] the FAR Council simply defined *de minimis* as the absence of a personal conflict of interest.

Certainly, administrative rule-making could tighten this, and other, definitions. But if the FAR Councils are truly unwilling to "create a mirror image of 18 U.S.C. § 208," on what legal structure will they tether new definitions? If 18 U.S.C. § 208 and its associated regulations are disfavored, then from whence shall guiding principles spring forth? Caselaw, as will be shown, is of little help. Regulations are

---

[136] *Id.*

[137] One must dig into the comments accompanying the rules to learn that the FAR Council likely meant "example" and "may" to denote 'including, but not limited to.' *See* Preventing Personal Conflicts of Interest for Contractor Employees Performing Acquisition Functions, 76 Fed. Reg. 68,017, 68,019 (Nov. 2, 2011).

[138] *See* FAR, 48 C.F.R. 3.1103(b) (2013); FAR, 48 C.F.R. 52.203-16(b)(6) (2013).

[139] FAR, 48 C.F.R. 3.1101 (2013) (definition of "Personal conflict of interest" has a *de minimis* exception); FAR, 48 C.F.R. 52.203-16(a) (2013).

[140] *See, e.g.,* 5 C.F.R. §§ 2634.301-2634.311 (2013) (describing various reporting thresholds for public disclosure reporters); 5 C.F.R. § 2634.907 (2013) (similarly for confidential reporters); 5 C.F.R. § 2635.204 (2013) (describing various exceptions to the gift rule).

[141] *See* Preventing Personal Conflicts of Interest for Contractor Employees Performing Acquisition Functions, 76 Fed. Reg. at 68,019 (circularly arguing against concerned respondents that "[i]n the definition of 'personal conflict of interest,' the regulation affords flexibility regarding de minimis interest, since it may be determined that a de minimis interest would not "impair the employee's ability to act" with the required objectivity.").

supposed to be built on underlying statutes. Without such a statute, it should come as little surprise how difficult crafting meaningful definitions is. A generally applicable criminal law would greatly assist regulators. Having a statutory foundation frames the issue and lets the regulators focus on their core competency—implementing law, not creating it.

B. Concerning Grantees, Why the Current Patchwork is Inadequate

As shown in *Town of Fallsburg*,[142] the government charged the Town Supervisor with crimes deriving from the underlying conflict of interest. But the government could not charge the Town Supervisor with the activity driving the criminal train: the conflict of interest itself. Had the Town Supervisor simply not acted so strenuously to further his inherent conflict of interest, no federal crime would have happened. That's because the underlying conflict itself is not criminal. And without the criminal conviction, the grant administrator's argument to support grant withholding before the Court of Claims would have been potentially much harder.

Figure 3, *infra*, demonstrates the only generally applicable law against grantee employees performing public acquisition while conflicted: a form requiring an assurance. This assurance is one of nineteen[143] or twenty[144] the applicant for the grantee provides. Many of these assurances, such as the one concerning conflicts of interest, speak of future, not current, compliance. Thus, a grantee can receive grant money without adequate safeguards developed or implemented by simply promising to do the spadework later.

More troubling is the lack of law underpinning the conflict of interest assurance. OMB grant circulars only apply conflict of interest rules to non-government grantees.[145] For government grantees, OMB circulars are silent on conflicts of interest. In fact, for government grantees only a single paragraph in a single standard form purports to protect against conflicted grantee employees using grant money to procurement goods and services from firms in which the employee has a financial interest. And even the most law abiding grantor could still allow conflicted public acquisition. For example, consider if a grantee *volunteer* awarded a contract to an entity with whom the volunteer had a financial interest. The OMB guidance existing speaks in terms of *employees*.[146] Without definitions, guidance, an underpinning

---

[142] 22 Cl. Ct. 633 (1991).

[143] *See* Office of Mgmt. & Budget, Exec. Office of the President, Standard Form 424B, *available at* http://apply07.grants.gov/apply/forms/sample/SF424B-V1.1.pdf (19 assurances).

[144] *See* Office of Mgmt. & Budget, Exec. Office of the President, Standard Form 424D, *available at* http://apply07.grants.gov/apply/forms/sample/SF424D-V1.1.pdf (20 assurances).

[145] *See* Office of Mgmt. & Budget, Exec. Office of the President, OMB Circular No. A-102 (Revised), Grants and Cooperative Agreements with State and Local Governments (1997), *available at* http://www.whitehouse.gov/omb/circulars_a102/ (conflict of interest unmentioned).

[146] *See* Office of Mgmt. & Budget, Exec. Office of the President, Standard Forms 424B, *supra* note 143, at ¶ 3 & Office of Mgmt. & Budget, Exec. Office of the President, Standard Forms

criminal law, or other legal foundation, a grant administrator may have a tough time finding the grantee violated the assurance, even under the deferential APA standard.[147] This would be especially true as, like under FAR Subpart 3.11, the grantee is only required to establish a system reasonably capable of, not actually, preventing conflicted public acquisition.

Like in the contracting community, a generally applicable criminal law can establish a clear norm against conflicted public acquisition in the grant community, regardless of employment or grantee status. OMB and other agencies could then craft their implementation of that law into their grant regulatory framework.

C. Concerning Parties to Other Transaction Agreements, Why the Current Patchwork is Inadequate

If protections against contractor employees performing conflict public acquisition are ineffectual and inadequate for grantee employees, then they are simply nonexistent for employees of other transaction agreements ("OTAs").

By way of background, OTAs is a catch-all term used to denote all the other transaction agreements that seem like a contract, grant, cooperative agreement, or mixture of those vehicles, but isn't any one of them particularly. The Congressional Research Service defined an OTAs as "a special type of vehicle or instrument used by federal agencies for research and development purposes . . . ."[148] This definition is slightly misleading. Indeed, OTAs are presently used largely for research and development purposes. However, the authority itself comes from Congress simply granting an agency authority conduct some form of public acquisition, as defined in this article,[149] outside the confines of a contract, grant, or cooperative agreement.[150]

---

424D, *supra* note 144, at ¶ 7.

[147] *See* 5 U.S.C. § 706 (2013) (setting the judicial review standard for agency decisions).

[148] L. Elaine Halchin, Cong. Research Serv., Other Transaction (OT) Authority 1 (2011), *available at* http://www.fas.org/sgp/crs/misc/RL34760.pdf.

[149] *See* Steven L. Schooner, *Desiderata: Objectives for a System of Government Contract Law*, 2 Pub. Procurement L. Rev. 103, 103 (2002) (citing integrity as "pillar" in public acquisition). *See also* Christopher R. Yukins, *Integrating Integrity and Procurement: The United Nations Convention Against Corruption and the UNCITRAL Model Procurement Law*, 36 Pub. Cont. L.J. 307 (2007) (arguing for greater integration of anti-corruption international law with the United Nations Commission on International Trade Law Model Law on Procurement of Goods, Construction, and Services). Integrity is especially important in the federal system given the large amount of money moving both out of the market as taxes and back into the market through contracts, grants, and other transactions. The government spent the following billions of dollars contracts and grants in the following fiscal years (format: FYXX, contracts, grants): FY10, $540.0, $614.3; FY11, $539.7, $567.0; FY12, $517.7, $538.6. USASpending.gov, *available at* http://www.usaspending.gov/explore. Money spent on other transaction is discussed separately later.

[150] *See* Nancy O. Dix, Fernand A. Lavalle & Kimberly C. Welch, *Fear and Loathing of Federal Contracting: Are Commercial Companies Really Afraid to do Business with the Federal Government? Should They Be?,* 33 Pub. Cont. L.J. 5, 23 (2003) (OTA "is defined in the negative, as an instrument *other than* a procurement contract, grant, cooperative agreement or [cooperative

In fact, the first Congressional grant of OTA authority placed no subject-matter limits on the authority.[151]

The exact extent and usage of OTAs is unknown. While some commenters have stated OTAs may include "many hundreds of agreements and billions worth of obligations . . . "[152] actual figures are unknown. At best, OTAs are a minor slice of the public acquisition pie, totaling no more than $7.1B in fiscal year 2012, $8.1billion in 2011, and $3.5B in 2010—a tiny fraction of the $1T-plus spent each of those fiscal years between contracts and grants.[153]

Significant users of OTAs include the Department of Defense ("DoD")[154] and Department of Homeland Security ("DHS").[155] However, both the Federal Aviation Administration ("FAA")[156] and the Transportation Security Administration ("TSA")[157] and have statutory other transaction power too. In 2004, Congress gave civilian agencies other transaction authority similar that of DoD's OTA authority until September 30, 2008.[158] This granted OTA authority to engage in research "to

---

research and development agreement].").

[151] *See* National Aeronautics and Space Act of 1958, Pub L. No. 85-568, § 203(b)(5), 72 Stat. 426, 430 (1958) (presently codified at 51 U.S.C. § 20113(e)) (authorizing NASA to "enter into and perform such contracts, leases, cooperative agreements, or other transactions as may be necessary . . . .").

[152] Richard L. Dunn, *Other Transactions—Another Chance?*, 50 NO. 5 Gov't Contractor ¶ 39 (2008).

[153] *See* USASpending.gov, http://www.usaspending.gov/explore (last visited May 1, 2014). Even these other transaction figures are inflated as they include payments to the United Nations, Red Cross, etc., that represent no public acquisition activity. However, controlling for those amounts is presently impossible.

[154] *See* 10 U.S.C. § 2371(a) (2013) (granting OTA authority "in carrying out basic, applied, and advanced research projects ."); 10 U.S.C. § 2373 (2013) (granting other transaction to buy "ordnance, signal, chemical activity, and aeronautical supplies, including parts and accessories, and designs thereof . . . consider[ed] necessary for experimental or test purposes . . . ."). For further information concerning DoD's usage of OTAs, *see* Under Secretary of Defense: Acquisition, Technology, and Logistics, *"Other Transaction" Authority (OTA) for Prototype Projects* (2001), *available at* https://acc.dau.mil/CommunityBrowser.aspx?id=37937.

[155] *See* 6 U.S.C. § 391(a)(1) (2013) (granting authority similar to that found in 10 U.S.C. § 2371). This authority will sunset on September 30, 2013; Consolidated and Further Continuing Appropriations Act, Pub. L. No. 113-6, § 525, 127 Stat. 198, 371 (Mar. 26, 2013). For further information concerning DHS's usage of OTAs, *see* U.S. Gov't Accountability Office, GAO-08-1088, Dep't of Homeland Security: Improvements Could Further Enhance Ability to Acquire Innovative Technologies Using Other Transaction Authority (2008).

[156] *See* 49 U.S.C. § 106(l)(6) (2013) (granting the FAA authority "to enter into and perform such contracts, leases, cooperative agreements, or other transactions as may be necessary . . . .").

[157] *See* 49 U.S.C. § 114(m)(1) (2013) (granting the TSA the same authority "provided to the Administrator of the Federal Aviation Administration under [49 U.S.C. § 106(l)]").

[158] *See* National Defense Authorization Act for Fiscal Year 2004, Pub. L. No. 108-136, § 1441, 117 Stat. 1392, 1673-4 (Nov. 24, 2003).

facilitate defense against or recovery from terrorism or nuclear, biological, chemical, or radiological attack . . . ," provided the Director of OMB authorized the project.[159]

An agency with OTA authority need not follow the FAR, OMB guidance, or a great many other laws one typically would think would apply to public acquisition. For example, the Anti-Kickback Act does not apply.[160] Nor does the prohibition against using appropriated funds to influence government decision-makers apply.[161] Many other laws do not apply.[162] This freedom makes OTAs potentially enticing to both parties wary of the complexities of government acquisition and government acquisition professionals with little funds to pay for additional FAR, grant, or cooperative agreement driven accounting, overhead, and compliance costs.[163] However, this freedom comes partially at the cost of many existing public policy protections. What is most troubling is that haphazard legal roulette replaced thoughtful public discourse on what laws apply, and do not apply, to OTAs. Thus, laws likely meant for general applicability, like the two cited at the beginning of this paragraph, are inapplicable not because of affirmative Congressional consideration and action but because the draftsmen likely simply did not think to list out yet another vehicle of public acquisition.

More broadly, one may wonder whether public acquisition occurs in OTAs. The short answer is nothing prevents it. Nothing prohibits an agency otherwise vested with appropriate OTA authority from using a private entity to accomplish or facilitate public acquisition.[164] For example, the National Aeronautics and Space Administration ("NASA"), FAA, and TSA all have general OTA authority. Their authority materially differs from that of DoD or DHS as their OTA authority is tied to research and development or prototyping activities. So while the risk of conflicted public acquisition may be low in OTAs, it does exist. Certainly, the anti-corruption patchwork quilt covers that risk, regardless of its size, the least.

---

[159] 41 U.S.C. § 1904(a)(1) (2013).

[160] *See* 41 U.S.C. § 52(2) (2013) (defining a "kickback" as value provided to any "prime contractor, prime contractor employee, subcontractor, or subcontractor employee . . . .").

[161] *See* 31 U.S.C. § 1352(a)(1) (2013) ("None of the funds appropriated by any Act may be expended by the recipient of a Federal contract, grant, loan, or cooperative agreement to pay any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with any Federal action . . . .").

[162] For a partial list of laws inapplicable to OTAs, *see* L. Elaine Halchin, *supra* note 148, at 19-22.

[163] *See, e.g.,* Susan B. Cassidy, Jennifer Plitsch & Stephanie H. Barclay, *Another Option in a Tightening Budget: A Primer on Department of Defense "Other Transactions" Agreements*, 48-SPG Procurement Law. 3, 3-10 (2013) (discussing the advantages of OTAs with nontraditional contractors and decreased federal funding); Richard L. Dunn, *supra* note 152 at ¶ 39 (similarly discussing advantages of OTAs).

[164] For example, *see* G & T Conveyor Co. v. Allegheny County, 2011 WL 5075353 (W.D.Pa. 2011) (not reported in F.Supp. 2d) (TSA provided defendant funds under a cost-sharing OTA to construct an in-line explosive detection system; defendant selected plaintiff as the contractor).

## IV. A GENERALLY APPLICABLE CRIMINAL LAW WOULD CREATE AND HARMONIZE LAW

This part discusses how a generally applicable criminal law would create and harmonize law concerning non-governmental employees engaging in public acquisition activities while having a personal conflict of interest.

The United States Court of Appeals of the Federal Circuit ("Federal Circuit") has oscillated on what a plaintiff alleging the taint of personal conflict of interest must show to gain review, given the absence of statutes and regulations. In contrast, the Government Accountability Office ("GAO") has adopted a totality of the circumstances analysis, using statutory and regulatory texts to guide, rather than underpin, their opinions. And the common law surrounding other transactions is almost entirely blank.

A generally applicable criminal law would give a label and analytical framework to a known, but not explicitly stated, wrong. All stakeholders, agencies, tribunals, contractors, grantees, non-government employees would benefit from a clear, concisely written, criminal statute demonstrating where the most fundamental of lines are drawn.

The first section will discuss the matter in context of the courts. The second section will discuss the matter in the context of GAO. The third and fourth sections briefly discuss the matter in the context of contract and grant performance, respectively. Finally, the fifth section discusses the matter in the context of other agreements.

### A. A Generally Applicable Criminal Law Would Harmonize Judicial Jurisprudence

The Federal Circuit is the appellate court for the boards of contract appeals and the Court of Federal Claims.[165] As such, its holdings are binding on these tribunals. For disputes and, since 1970 in *Scanwell Laboratories, Inc. v. Schaffer*,[166] protests the Federal Circuit (or its predecessors in interest prior to its establishment in 1982), has reviewed agency contracting actions against an "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law,"[167] standard. How a personal conflict of interest alleged to have tainted a government decision juxtaposes against that standard has not always been clear.

---

[165] *See* 28 U.S.C. 1295(a)(3), (10) (2013) (granting the Federal Circuit appellate jurisdiction over the stated entities).

[166] 424 F.2d 859 (D.C. Cir. 1970).

[167] *Id.* at 874 (quoting 5 U.S.C. § 706(2)(A)). This bootstrapped standard of review was later statutorily appended to the trial claims courts' jurisdiction. *See* Administrative Dispute Resolution Act of 1996, Pub. L. No. 104-320, § 12(a)(3), 110 Stat. 3870, 3875 (Oct. 19, 1996) (codified at 28 U.S.C. § 1491(b)(4)).

In 1981, a three judge panel of the Court of Claims in *Baltimore Contractors, Inc.*[168] split three ways on whether the trial court must grant finality to a 1975 contract appeal board's decision under the Wunderlich Act[169] when the board members are perceived to have conflicts of interest.[170] The majority opinion held that perception, absent any proof or violation of law, was sufficient to disregard the Wunderlich Act's stamp of finality typically assigned to board decisions.[171] The court remanded the matter to a trial judge for a *de novo* opinion on the complete record without deference to the board's decision. The concurring judge concurred in result only, stating the Fifth Amendment[172] guaranteed the contractor an impartial board.[173] The dissenting judge took issue with both opinions.[174] The dissent argued the board's superior steering committee could allow such personal conflicts. The dissent thought the organization should able to internally administer its contract dispute affairs without judicial interference provided determinations were not "fradulent or capricious or arbitrary or so grossly erroneous as necessarily to imply bad faith, or is not supported by substantial evidence."[175] Thus *Baltimore Contractors* established precedence for looking at the totality of the circumstances surrounding the perceived fairness of government action rather than requiring a specific statutory or regulatory violation.

In 1983, the then recently constituted Federal Circuit partially walked *Baltimore Contractors* back. In *C.A.C.I., Inc.-Fed.,*[176] the Federal Circuit reversed a Claims Court decision[177] enjoining contract award based on perceived personal

---

[168] 643 F.2d 729 (Cl. Ct. 1981).

[169] *See* Wunderlich Act of 1954, Pub. L. No. 83-356, 68 Stat. 81 (May 11, 1954) (codified then at 41 U.S.C. §§ 321-2). The Wunderlich Act was designed to abrogate the Supreme Court case *United States v. Wunderlich*, 342 U.S. 98 (1951). In *Wunderlich*, the Supreme Court held a reviewing court could not overturn an agency's final decision on government contractual matters absent fraud. Congress acted a few years later to state the agency's decision "shall be final and conclusive unless the same is fraudulent or capricious or arbitrary or so grossly erroneous as necessarily to imply bad faith, or is not supported by substantial evidence." Wunderlich Act, Pub. L. No. 83-356, § 1. The Wunderlich Act was later apparently repealed upon the enactment of the Contract Disputes Act of 1978, Pub. L. No. 95-563, § 14(i), 92 Stat. 2383, 2391 (Nov. 1, 198), though one must read the legislative history for confirmation, *see* S. Rep. No. 95-1118, at 34 (1978).

[170] *See* Baltimore Contractors, Inc., 643 F.2d 729 (Cl. Ct. 1981). The board was specially created to hear disputes arising from Architect of the Capitol contracts for the construction of the Rayburn House Office Building. *Id*. at 729-32. The board members were exclusively GAO employees appointed to serve at the pleasure of the steering committee, shared office space and administrative support with contract administration personnel, and executed other duties while serving on the board. *Id*. at 731-3.

[171] *See id.* at 733-4.

[172] *See* U.S. Const. amend. V ("No person shall . . . be deprived of life, liberty, or property, without due process of law . . . .").

[173] See *Baltimore Contractors, Inc*., 643 F.2d at 735-6.

[174] *See id.* 736-47.

[175] *Id.* at 734.

[176] 719 F.2d 1567 (Fed. Cir. 1983).

[177] It appears the same trial judge, Judge Spector, penned both trial decisions appealed in *Baltimore Contractors, Inc.* and *C.A.C.I., Inc.-Fed*. *See id*. at 1569; *Baltimore Contractors, Inc.,*

conflicts of interest and alleged violations of personnel ethics regulations.[178] At issue were loose employment opportunities discussed between the successful offeror and members of the source selection team prior to contract award. The Federal Circuit declined to utilize the established fourteen general principles of public service established in regulations,[179] first found in President Bush's executive order,[180] as guidance. Rather, the Federal Circuit stated such regulations "merely provide[d] general standards to guide government employees in the performance of their duties. It does not create specific and precise standards, the violation of which would justify enjoining the [government] from awarding a contract."[181] As no specific law prohibiting these loose discussions then existed, the court applied the deferential APA analysis and held the award was not "arbitrary, capricious, [or] an abuse of discretion."[182] Thus, the Federal Circuit signaled the need for plaintiffs to allege a violation of a specific ethics law or regulation complaining of a conflict of interest rather than a general policy against them.

The Federal Circuit decided *C.A.C.I., Inc.-Fed.* before the FAR became effective April 1, 1984.[183] The FAR included a regulation, FAR 3.101-1, that directed contracting officers to "avoid strictly any conflict of interest or even the appearance of a conflict of interest in Government-contractor relationships."[184] Thus, the question became whether this rather policy-orientated regulation was specific enough to drive a conflict of interest allegation under *C.A.C.I., Inc.-Fed.*, thus signaling a shift back toward the majority rationale in *Baltimore Contractors*. The only Federal Circuit case addressing this question is *Galen Med. Assoc., Inc*.[185] Here, the protestor alleged certain government employee proposal evaluators had a conflict of interest because the successful offeror listed them as past performance references.[186] The court found "no code section forbid[ding] an agency official listed as one to validate

643 F.2d at 729.

[178] *See C.A.C.I., Inc.-Fed.*, 719 F.2d at 1581.

[179] Currently, the fourteen principles are found at 5 C.F.R. § 2635.101(b) (2013).

[180] *See* Exec. Order No. 12,731, § 101, 55 Fed. Reg. 42,547, 42547 (Oct. 17, 1990).

[181] *C.A.C.I., Inc.-Fed*., 719 F. 2d at 1581. *See also* United States v. Mississippi Valley Generating Co., 362 U.S. 939 (1960) (affirming voiding of contract on the basis of contractor conflict of interest violating criminal statute despite no charges against individual).

[182] *C.A.C.I., Inc.-Fed*, 719 F. 2d. at 1581-2. Please note this case was decided before the adoption of the Procurement Integrity Act. *Compare* Office of Federal Procurement Policy Act Amendments of 1988, Pub. L. No. 100-679, § 6, 102 Stat. 4055, 4063 (Nov. 17, 1988), *with C.A.C.I., Inc.-Fed*, 719 F. 2d. 1567 (decided Oct. 28, 1983).

[183] *Compare* Establishing the Federal Acquisition Regulation, 48 Fed. Reg. 42,102, 42,108 (Sept. 19, 1983) (regulations effective Apr. 1, 1984), *with C.A.C.I., Inc.-Fed.*, 719 F. 2d 1567. (decided Oct. 28, 1983).

[184] Establishing the Federal Acquisition Regulation, 48 Fed. Reg. 42,102, 42,108 (Sept. 19, 1983). This language has not changed in the intervening years. *Compare id.*, *with* FAR, 48 C.F.R. 3.101-1 (2013).

[185] 369 F.3d 1324 (Fed. Cir. 2004).

[186] *Id.* at 1335.

past performance reference from serving as an evaluator."[187] Then, the court went further: "even to the extent the regulations require that any conflict of interest or even the appearance of a conflict of interest in government-contractor relationships be avoided, [FAR 3.101-1], [the protestor] has failed to show any potential symbiotic relationship between the technical evaluators and" the successful offeror.[188] Whether the Federal Circuit truly meant to elevate the policy stated in FAR 3.101-1 beyond "merely provid[ing] general standards to guide government employees,"[189] is not entirely clear. The Court of Federal Claims has taken it that way. [190] But the Federal Circuit's phraseology sounds like the court is answering a question not asked. Thus, a future court may hew toward the clear holding of *C.A.C.I., Inc.-Fed.* rather than this extra argument asked and answered in *Galen Med. Assoc.*

While these cases dealt chiefly with conflicts of interest on the part of government public acquisition actors, one need have little imagination to apply the lessons to a non-governmental actor. The Federal Circuit appreciates hard and fast law on which to ground a conflict of interest analysis. The lack of such a law for non-governmental actors leaves only the dicta in *Galen Med. Assoc.* to buttress the usage of FAR 3.101-1. Failing that, *C.A.C.I., Inc.-Fed.* suggests that without a clear law prohibiting a conflict of interest amongst non-governmental actors, such conflicts of interest are poor vehicles for a bid protest or appeal.

### B. A Generally Applicable Criminal Law Would Further Improve GAO Bid Protest Jurisprudence

In contrast to the Federal Circuit and its subordinate tribunals, GAO is less tied to specific statutes or regulations.[191] When a conflict is alleged, GAO is more likely to adopt a totality of the circumstances approach, though not with those specific words. GAO's analysis typically starts with whether the person alleged to have a conflict has both an official role in the procurement and a personal stake in the

---

[187] *Id.* at 1336.

[188] *Id.*

[189] C.A.C.I., Inc.-Fed. v. United States, 719 F.2d 1567, 1581 (Fed. Cir. 1983).

[190] *See e.g.,* MORI Assoc., Inc. v. United States, 102 Fed. Cl. 503, 525 (2011) ("[T]he Federal Circuit . . . has recognized that [FAR 3.101-1] imposes requirements upon procurement officials.") (citing *Galen Med. Assoc., Inc.*, 369 F.3d at 1336 ). Research did not disclose any boards of contract appeals cases concerning conflicted acquisition support services.

[191] *See, e.g.,* Sci. Pump Corp., B-255737, 94-1 CPD ¶ 246 (Comp. Gen. Mar. 25, 1994) (stating whether employee "violated 18 U.S.C. § 208 and related regulations is not within the purview of our bid protest regulations . . . . Our review . . . is limited to whether the applicable procurement regulations prohibit" the awardee from winning the contract given the employee's actions); Development Assoc. Inc., B-187756, 77-1 CPD ¶ 310 (Comp. Gen. May 5, 1977) ("There is no statutory or regulatory authority for our office to issue formal opinions on conflict of interest questions . . . . Notwithstanding our position . . . we have, on occasion, offered views about considerations bearing on alleged violations of standards of conduct as they related to propriety of particular procurement.").

outcome.[192] If such competing interests are found, GAO will then require "convincing proof" that those individuals "exerted improper influence in the procurement on behalf of the awardee, or against the protestor."[193] The GAO conducts a fact-intensive analysis to determine if the allegation is substantiated and, if so, how the conflict impacted the procurement.[194] The GAO also gives deference to agency decisions

[192] *See, e.g.,* TPL, Inc., B-297136, 2006 CPD ¶ 104 (Comp. Gen. June 29, 2006) (listing various times the inquiry has been applied).

[193] Phacil Inc., B-406628, 2012 CPD ¶ 202 (Comp. Gen. July 5, 2012). *See also* Advanced Sys. Tech., Inc.; Eng'g & Prof'l Serv., Inc., B-241530, 91-1 CPD ¶ 153 (Comp. Gen. Feb. 12, 1991) (protest alleging procurement officials had various personal and familial conflicts of interest denied because protestor lacked proof of improper act).

For a time, GAO had a series of cases where GAO, arguably, did not require convincing proof of improper influence. In reviewing protests on public-private competitions, *see* Office of Mgmt. & Budget, Exec. Office of the President, Cir. No. A-76 Revised (2003), *available at* http://www.whitehouse.gov/omb/circulars_a076_a76_incl_tech_correction#1. GAO held the mere presence of the same agency employees (and supporting contractors, if applicable) both running and competing in the same competition violated FAR 3.101-1. *See, e.g.,* Dep't of the Navy—Reconsideration, B-286194.7, 2002 CPD ¶ 76 (Comp. Gen. May 29, 2002) (protest sustained when same agency employees and support contractor wrote A-76 competition performance work statement); DZS/Baker L.L.C.; Morrison Knudsen Corp., B-281224, 99-1 CPD ¶ 19 (Comp. Gen. Jan. 12, 1999) (protest sustained when 14 of 16 A-76 competition evaluators occupied positions subject to the A-76 study).

The GAO used FAR 3.101-1 to establish the standard of conduct required. Then, GAO would apply organizational conflict of interest analysis and essentially if one of the bidders, the government, was writing its own specifications. *See, e.g., DZS/Baker*, 99-2 CPD ¶ 19, 2 ("FAR subpart 3.1 does not provide specific guidance regarding situations in which government employees, because of their job positions or relationships with particular government organizations, may be unable to render impartial advice to the government. However . . . FAR subpart 9.5 addresses analogous situations involving contractor organizations. Accordingly, although FAR subpart 9.5, by its terms, does not apply to government agencies or employees, we believe that in determining whether an agency has reasonably met its obligation to avoid conflicts under FAR § 3.101-1, FAR subpart 9.5 is instructive in that it establishes whether similar situations involving contractor organizations would require avoidance, neutralization or mitigation.").

Once OMB Cir. A-76 was revised to prohibit government employees from being on both sides of an A-76 competition, borrowing from organizational conflict of interest law became unnecessary. *See* CR Assoc., Inc., B-297686, 2006 CPD ¶ 61 (Comp. Gen. Mar. 7, 2006) (A-76 competition protest denied when agency used disinterested employees to run competition, no improper influence found), IT Facility Serv.-Joint Venture, B-285841, 2000 CPD ¶ 177 (Comp. Gen. Oct. 17, 2000) (additionally, potential conflict of interest found "insignificant" when one evaluator was married to a government employee whose position was subject to the A-76 competition). For more background on GAO's analysis during that time, *see* U.S. Gov't Accountability Office, Letter to OGE Regarding Conflicts of Interest in A-76 Cost Comparisons, B-281224.8, 99-2 CPD ¶ 103 (Comp. Gen. Nov. 19, 1999).

[194] *See* Textron Marine Sys., B-255580, 94-2 CPD ¶ 63 (Comp. Gen. Aug. 2, 1994) (fact-intensive analysis regarding Navy civilian employee's involvement with a procurement his future employer won).

allowing a conflict when the contracting officer has investigated, documented, and taken reasonable action to mitigate the conflict's effects.[195]

For example, in *Celadon Laboratories*, GAO was confronted with an allegation of conflicts of interest amongst non-government actors providing acquisition support services for the agency.[196] Four of four non-government Small Business Innovation Research Phase I proposal technical evaluators found the protestor's proposal, based on siLNA technology, technically unacceptable.[197] The protestor alleged all four non-government evaluators had conflicts of interest because each "work for, or are associated with . . . siRNA technology, a technology that Celadon, without rebuttal, asserts was directly competitive with the [siLNA] technology it offered in its proposal . . . ."[198]

Despite being untimely, GAO found the "significant issue"[199] exception applied.

> We need not resolve whether this procurement was [timely] . . . within the meaning of our timeliness rules because we find that this protest is appropriate for consideration under the significant issue exception to our timeliness rules. . . . The issue here—the application of conflict of interest regulations to peer review evaluators in SBIR procurements—is not one that we have previously decided and is one that can be expected to arise in future SBIR procurements.[200]

The agency argued each evaluator had received training on conflicts of interest and certified he or she did not have any conflicts of interest.[201] Furthermore, the contracting officer verified each evaluator certified he or she had no conflict of interest and found no evidence of bias in the evaluation.[202] The GAO found this investigation insufficient and sustained the protest.

---

[195] *See* Battelle Mem'l Inst., B-278673, 98-1 CPD ¶ 107 (Comp. Gen. Feb. 27, 1998) (successful offeror proposed using a certain government facility to conduct testing and government employees of that facility were evaluating the proposals, contracting officer identified and evaluated the potential conflict of interest and found the conflict insignificant, GAO found contracting officer's actions and determinations reasonable).

[196] *See* Celadon Lab., Inc., B-298533, 2006 CPD ¶ 158 (Comp. Gen. Nov. 1, 2006).

[197] *See id.* at 2.

[198] *Id.*

[199] *See* 4 C.F.R. § 21.2(c) (2013) (The GAO may consider an untimely protest when the protest "raises issues significant to the procurement system . . . .").

[200] Celadon Lab., Inc., 2006 CPD ¶ 158, 4.

[201] *See id.* at 5.

[202] *Id.*

> While it is true that the [agency] regulations contemplate a self-assessment by evaluators as to whether they think they have a real conflict of interest, the regulations do not contemplate that a self-certification by the evaluator is all that is ever needed to satisfy the requirement that he or she does not have a real conflict of interest, particularly where, as here, specific and colorable allegations of a real conflict of interest on the part of the evaluators were brought to the attention of cognizant agency officials. . . . While we do not decide whether the evaluators here had real conflicts of interest, the record shows that the agency failed in its obligation to determine whether these individuals' employment caused them a real conflict of interest that could bias their evaluation . . . .[203]

Taking this protest one step further illustrates why adoption of a criminal law regarding this type of conduct could be helpful. What if the contracting officer had done more investigation and discovered the underlying relationships? Against what standard would the contracting officer gauge the agency's tolerance for a conflict? In this case, the contracting officer had a particular agency regulation concerning conflicts of interest.[204] However, the contracting officer's utilization of this fairly developed and specialized regulation along with independent documented investigation did not save the procurement. Consider the case of a contracting officer without the benefit of that agency's particular regulations. Against what legal standards is the conflict to be investigated? If the conflict occurred in the past, what level of "conflict" can the contracting officer find acceptable? And what chance does that decision, not grounded in a directly applicable law or policy, have to stand in a protest at GAO? Without a guide,[205] the contracting officer is left with "[t]he general rule . . . to avoid strictly any conflict of interest or even the appearance of a conflict of interest in Government-contractor relationships,"[206] a standard the Court of Federal Claims does not utilize and GAO cites obligatorily before diving into the nuts and bolts of the matter. A generally applicable criminal public acquisition conflict of interest law would give all stakeholders a foundation on which to guide (and judge) their actions.

### C. Clear Standard for Contract Performance and Administration

In all likelihood, most contractor employee conflict of interest issues will never reach beyond contract performance and administration. Contracting officers, project managers, compliance officers, and counsel will review specific questions against meager and grey jurisprudence and guidance.[207] A fundamental criminal law

---

[203] *Id.* at 5.

[204] *See id.* at 7.

[205] *See infra* Figures 2 and 3 for potential sources of guidance.

[206] FAR, 48 C.F.R. § 3.101-1 (2013).

[207] What little has been written about FAR Subpart 3.11 has generally focused on explaining the

can clarify the lines for all stakeholders, thus bringing a measure of structure and predictability in what could otherwise be a race to the bottom.

For contractors, a generally applicable criminal law would give something to further motivate employees. One commentator has already hinted at information asymmetry between the contractor and contractors' employees concerning potential personal conflicts of interest.[208] The same asymmetry exists in the federal financial disclosure system between supervisors and their filing employees. However, federal filers have the additional motivation to make full disclosures because doing otherwise risks violating federal criminal law.[209] Creation of a similar law would serve similar purposes thus driving more disclosures and greater achievement of the law's intent.

Additionally, a generally applicable criminal law would give structure to the conflict of interest analysis FAR Subpart 3.11 requires contractors to accomplish. Contractors would have clearer standards of what constitutes an impermissible conflict of interest and, thus, what is, essentially, a permissible or, in FAR Subpart 3.11 parlance, a *de minimis* conflict of interest. Contractors would have a better idea what their compliance efforts will involve and thus need to build in less risk costs into their proposal. And contractors would have a better chance at defeating auditors and others second-guessing their decisions because a generally applicable criminal law would set the standard. The onus would be on the agency to, through rule-making or clause, raise the generally applicable standard.

D. Clear Standard for Grant Performance and Administration

The Supreme Court has recognized a grantee employee can hold "a position of public trust with official federal responsibilities: allocating federal resources, pursuant to complex statutory and regulatory guidelines, in the form of . . . contracts."[210] The logic behind this statement is clear when one considers the "official" federal power a grantee employee can exercise. Grantees largely operate independently, awarding federally funded contracts outside the FAR and many other federal regulatory controls. The combination of money and minimal oversight and control can breed conflicts of interest.

---

rule though some writings, s*ee, e.g.,* Keith R. Szeliga & Franklin C. Turner, *supra* note 100, at 6 ; David J. Ginsberg & Robert R. Bohn, *supra* note 134, at 11, have noted various issues.

[208] *See* Keith R. Szeliga & Franklin C. Turner, *supra* note 102, at 5-6 (noting the contractor's duty extends to informing employees of their obligation to report financial interests of members of their households, not to actually ensure the employees actually comply).

[209] *See* 18 U.S.C. § 208 (2013). Federal employees also must certify their disclosures are true and correct to the best of their knowledge. Falsely certifying can drive a false statement violation. 18 U.S.C. § 1001 (2013). Uniform personnel additionally have criminal liability under the Uniform Code of Military Justice. 10 U.S.C. § 907 (2013).

[210] Dixson v. United States, 465 U.S. 482, 497 (1984) (affirming federal bribery convictions of executives of a private nonprofit program administering a federal housing grant).

The guidance provided does little to appraise grantees and grant officers where the line is and whether it has been crossed. The assurance requires the grantee's future system to "prohibit employees from using their positions for a purpose that constitutes or presents the appearance of personal or organizational conflict of interest, or personal gain."[211] What is an "appearance" of a conflict? Is the test subjective or objective or both? What if one grant officer uses one test and another uses another? If so, is the grant officer acting "arbitrar[ily] , capricious[ly] . . . or otherwise not in accordance with the law," or abusing his or her discretion?[212] A generally applicable criminal law could set the floor of such an analysis. Certainly, OMB or the granting agency could prohibit conflicts beyond what the statute allows. But without a generally applicable criminal law to initially ground the regulations, the bare regulations serve as the primary substantive authority. Regulations make more sense when read against a statutory framework. A generally applicable criminal law could give those regulations the necessary framework on which to build their regulatory anticorruption house.[213]

### E. Clear Standard for Other Transaction Agreement Performance and Administration

The category of OTAs is a prime example how a generally applicable criminal law against conflict public acquisition could form a single standard across all vehicles of public acquisition, even the ones that defy an affirmative label.

Right now, there is no standard at all regarding how private persons should conduct public acquisition under an OTA. No statute applies. No regulation applies. No rule applies. No policy exists.[214] Like for contracts, the public relies on the individual agreement officer or activity to foresee the potential risk and insert a preventative clause. This is especially unlikely because OTAs are supposed to be free of "unnecessary" requirements and thus more enticing for private participation.[215]

---

[211] Office of Mgmt. & Budget, Exec. Office of the President, Standard Forms 424B, *supra* note 143, at ¶ 3; Office of Mgmt. & Budget, Exec. Office of the President, Standard Forms 424D, *supra* note 144, at ¶ 7.

[212] 5 U.S.C. § 706(2)(A) (2013). *See also* Bennett v. New Jersey, 470 U.S. 632, 646 (1985) (holding, in part, that when an agency "has properly concluded that funds were misused under the legal standards in effect when the grants were made, a reviewing court has no independent authority to excuse repayment based on its view of what would be the most equitable outcome.").

[213] For example, the conflict of interest prohibition at FAR 3.101-1 clearly exceeds the scope of 18 U.S.C. § 208. By doing so, regulation communicates the expectation of a higher standard of conduct than what the underlying criminal law provides.

[214] *See, e.g.,* Under Secretary of Defense: Acquisition, Technology, and Logistics, *"Other Transaction" Authority (OTA) for Prototype Projects* (2001), *available at* https://acc.dau.mil/CommunityBrowser.aspx?id=37937 (no discussion of conflicts of interest or ethics in writing an OTA).

[215] *See generally* Nancy O. Dix, Fernand A. Lavalle & Kimberly C. Welch, *supra* note 148, at 27.("The latitude afforded to the Government by [OTAs] enables the sovereign to attract contractors that traditionally would not, or could not, do business with the Government.").

If one accepts that public acquisition should be free of personal conflicts of interests, the employment status of the actors and the public acquisition vehicle should not matter. Only the act of acquiring goods or services using the public fisc should matter. Enacting a generally applicable criminal law prohibiting conflicted public acquisition establishes a norm applicable to all forms of public acquisition, to include OTAs.

## V. ADDRESSING OTHER POTENTIAL COUNTERARGUMENTS

This part addresses a few potential arguments, not previously discussed, against the proposed generally applicable criminal law. Obviously, more concerns than those noted below exist. The intention here is to address what the author perceives to be significant counterarguments that have yet to be directly addressed.

### A. Another Criminal Law Will Simply Increase Costs

For this argument to make sense, one of two things must exist. First, private entities must currently, or reserve the right to someday, assign personally conflicted private persons to perform delegated or tasked public acquisition activities. This would mean the proposed generally applicable criminal law would remove present personnel flexibility thus driving increased personnel costs. If this is truly the case, then perhaps the necessity of the proposed law becomes obvious. But more likely the talent pool contains few truly conflicted persons.

The other fact that must exist for is this argument to make sense is that private entities will incur additional administrative monitoring costs to ensure an employee's conduct, being potentially criminal, does not cause organizational legal liability.[216] This merits further consideration.

For contractors, current FAR requirements suggest many potential compliance costs the proposed generally applicable criminal law would drive are already being incurred. Consider that FAR Subpart 3.11 already requires the contractor to establish a compliance and monitoring system concerning personal conflicts of interest.[217] The contractor need not develop a parallel system. The contractor could design the FAR Subpart 3.11 mandated compliance and monitoring system to accommodate further safeguards the proposed generally applicable criminal law

---

[216] *See, e.g.,* 18 U.S.C. § 2 (2013) (aiding and abetting criminal statute, affixing criminal liability for another's conduct when the defendant "aids, abets, counsels, commands, induces or procures" the crime's commission); 18 U.S.C. § 1031 (2013) (major frauds criminal statute, requires "intent—(1) to defraud the United States; or (2) to obtain money or property by means of false or fraudulent pretenses, representations, or promises," in connection with a grant or contract valued over $1M); United States v. President & Fellows of Harvard Coll., 323 F. Supp. 2d 151, 190-4 (D. Mass. 2004) (holding the parent organization not liable under the False Claims Act because parent organization did not know, and was not reckless in not knowing, that certain employees had conflicts of interest).

[217] *See* FAR, 48 C.F.R. 52.203-16(b)(1) (2013) (requiring the contractor to establish a system to "screen covered employees for potential personal conflicts of interest . . . .").

inherently suggests. For example, the existing system could require affirmative disclosures of potential conflicts, like is done under the OGE regulations.[218] This would provide the contractor notice of all potential conflicts rather than relying on the employee to correctly conduct his or her own analysis—an analysis already fraught with subjectivity and discretion. In constructing such a system, the contractor could adopt and tailor large swaths of the OGE rules to minimize development costs.

Dovetailing FAR Subpart 3.11 compliance with compliance safeguards likely necessary from the proposed generally applicable criminal law is only a partial answer. Some contractors provide acquisition support services as a commercial service and thus will not have FAR 52.203-16 in their contract.[219] Additionally, grantees and OTA parties will likely lack sophisticated disclosure requirements.[220] So what about these receiptants of federal funding who accomplish public acquisition?

Unfortunately, additional costs might be necessary for those entities. Legal counsel will likely advise some sort of disclosure form and review process to ensure the organization is not facilitating a crime. However, freely available OGE forms and regulations can greatly simply the disclosure task. Locally implemented bright line rules can also reduce costs. For example, not granting waivers and not allowing one accomplishing public acquisition to touch any contract in which that person has an interest at all can further reduce the compliance resources necessary. Balancing tests and discretion take time and resources. It is doubtful the talent pool is so shallow that such things are truly necessary. Additionally, contractors without the FAR 52.203-16 clause in their contracts and all grantees should be accomplishing basic conflict of interest screening anyway to minimize False Claims Act[221] liability exposure or jeopardize their funding.[222]

---

[218] *See generally* 5 C.F.R. § 2634.901-909 (2013) (requirements for confidential disclosure of financial information).

[219] *See* Preventing Personal Conflicts of Interest for Contractor Employees Performing Acquisition Functions, 76 Fed. Reg. 68,017, 68,025 (Nov. 2, 2011) (excluding commercial items from FAR Subpart 3.11).

[220] Even many governmental grantees will lack conflict of interest disclosure requirements. For an initial review of financial disclosure requires for procurement officials amongst the various states, *see* Your State, State Integrity Investigation, http://www.stateintegrity.org/your_state (last visited Mar. 24, 2013) (click on the desired state, then the button labeled "Procurement," then indicator 8.1, then number 206 entitled "[i]n law, there is a mechanism that monitors the assets, incomes, and spending habits of public procurement officials;" within the "Sources" box is often a legal citation to direct further research). *See also* Danielle M. Conway, State and Local Government Procurement (American Bar Association 2012) (chapter 12 concerns ethics in state procurement governance structures).

[221] *See* United States v. Sci. Applications Int'l Corp., 626 F.3d 1257 (D.C. Cir. 2010) (holding a contractor with organizational conflicts of interest who submits vouchers for payment of advisory services can be civilly liable under the False Claims Act when conflict-free advisory services were material to the government's decision to pay); United States ex rel. Harrison v. Westinghouse Savannah River Co., 176 F.3d 776 (4th Cir. 1999) (similarly holding an organizational conflict of interest can substantiate a False Claims Act case).

[222] *See* Town of Fallsburg v. United States, 22 Cl. Ct. 633 (1991) (grantee lost grant after agent

Finally, private entities should ensure their compliance is proportional to the legal risk generated. Advising legal counsel and compliance officers who believe the proposed criminal law would significantly impact their organization should already have much of this structure presently established given the risk of False Claims Act litigation. The number of False Claims Act cases the Department of Justice filed far exceeds by many magnitudes the number of prosecutions occurring under the proposed criminal law's existing cousin, 18 U.S.C. § 208.[223] Therefore, entities should ensure their compliance efforts remain focused on False Claims Act liability risk and only make tweaks necessary to accommodate any new risk the proposed generally applicable criminal law presents. Therefore, one should not expect this law to independently drive many new costs.

B. New Criminal Law Unnecessary to Defend the Government's Interests

The small numbers of 18 U.S.C. § 208 cases[224] filed and the lack of data demonstrating private persons are accomplishing conflicted public acquisitions begs the question, why such a law is needed? This argument is especially tempting given the apparent ability of the False Claims Act to reach entities who enable conflicted employees to perform public acquisition. The prospect of statutory and treble damages[225] arguably motivates many already. Additionally, contractors have the business ethics rule[226] and FAR Subpart 3.11[227] already applicable. The responsive steps those entities have already taken have arguably generated the second and third order effects likely reducing the risk of conflicted public acquisition.

In parts III and IV, this article touched upon many structural improvements to the existing anti-corruption regime a generally applicable criminal law could drive. They need not be individually repeated here. However, it bears repeating that a criminal law against any person's conflicted public acquisition will create a foundation upon which regulators, agencies, and others can harmonize to and build upon. Harmonization can reduce transaction costs and provide objective standards upon which private entities can better estimate their compliance costs. This can,

---

for grantee engaged in public acquisition with an organization in which the agent was financially interested).

[223] The Department of Justice charged few defendants with violating 18 U.S.C. § 208. *See* Bureau of Justice Statistics, Dep't of Justice, http://bjs.gov/fjsrc/tsec.cfm (last visited Mar. 24, 2013) (FYXX, number of defendants: FY10, 7; FY09, 4; FY08, 4; FY07, 6; FY06, 6; FY05, 8). During that same time frame, the Department of Justice investigated far more False Claims Act cases. *See* Civil Div., Dep't of Justice, http://www.justice.gov/civil/docs_forms/C-FRAUDS_FCA_Statistics.pdf (list visited Apr. 3, 2013) ("new matters" means "newly received referrals investigations, and qui tam actions.") (FYXX, number of False Claims Act "new matters": FY10, 715; FY09, 565; FY08, 541; FY07, 495; FY06, 456; FY05, 511).

[224] *See id.*

[225] *See* 31 U.S.C. § 3729(a) (2013).

[226] *See* FAR, 48 C.F.R. subpart 3.10 (2013).

[227] *See* FAR, 48 C.F.R. subpart 3.11 (2013).

in turn, lead to lower prices both from knowing what the standard truly is up front and not having to price the risk of an especially conservative contracting, grant, or agreement officer demanding more compliance within the gray.

The lack of horror stories means little.[228] Already little prosecution occurs under 18 U.S.C. § 208—but that does not mean it should be repealed. The proposed generally applicable criminal law's larger value is how it creates the base upon which everyone can build. Its ability to serve as a prosecution charge is an important systematic safety valve for especially bad actors, but that is not the law's core value. Additionally, little information exists concerning the extent of private persons performing public acquisition services while conflicted. Thus, the lack of horror stories may reflect a lack of information more than a lack of existence. And regardless of one's agreement with that statement, Figure 2 demonstrates Congress and agencies apparently feel there is a significant problem—otherwise why, especially for the less politically driven agencies, would the catalogued controls exist if not to address a need?

More fundamentally, why should private employees not be potentially held criminally liable for performing public acquisition with an entity in which he or she has a financial interest? Federal employees can be imprisoned, fined, and labeled a felon[229] for that, and more, conduct. Why should others engaging in the same conduct be simply reassigned or, at worst, fired—assuming their supervision even cares?[230] Why should investigators and prosecutors have to find criminal conduct derivative of the conflict of interest before they can file charges? After all, the FAR already requires a contractor to inform the government when "the Contractor has credible evidence that a principal, employee, agent, or subcontractor of the Contractor has committed . . . [a] violation of Federal criminal law involving . . . conflict of interest . . . ."[231] Since its enactment in December of 2007, this language has been essentially worthless as no such law exists![232] A generally applicable criminal law as proposed would fill that void.

---

[228] *See* Administrative Conference of the United States, *supra* note 4, at 5 ("Whether or not there is any widespread pattern of ethical abuses, the existence of significant ethical *risks* can erode public confidence in the government procurement process and in the government itself.").

[229] *See* 18 U.S.C. § 216(a)(2) (2013) (establishing the penalty for willful violations of 18 U.S.C. § 208). Less than willful violations would be a misdemeanor. *See* 18 U.S.C. § 216(a)(1).

[230] Suspension or debarment of the employee is possible. *See* FAR, 48 C.F.R. 9.407–2(a)(9) (2013) (making commission of acts "indicating a lack of business integrity or business honesty that seriously and directly affects the present responsibility" a ground for suspension). *See* FAR, 48 C.F.R. 9.406–2(a)(5) (2013) (making commission of acts "indicating a lack of business integrity or business honesty that seriously and directly affects the present responsibility" a ground for debarment).

[231] FAR, 48 C.F.R. 52.203–13(b)(3)(i)(A) (2013). *See also* FAR, 48 C.F.R. 3.1003(a)(2) (2013) (stating any contractor not reporting such conduct may be suspended or debarred).

[232] The drafters and the OGE were oddly concerned with organizational conflicts of interest rather than personal conflicts of interest. *See* Contractor Code of Business Ethics and Conduct, 72 Fed. Reg. 65,873, 65,877 (Nov. 23, 2007) (referencing a Department of Education Inspector General's

## VI. CONCLUSION

For almost a hundred years, from 1863 to 1962, the law did not care who a person worked for or how that person's employer got the work to start with when guarding against at least some of the acts constituting public acquisition. When someone used a federal acquisition vehicle entrusted to them to enrich themselves, the law clearly said no.

But that was undone in 1962. Without reason, cause, or perhaps even knowledge or intent. In its place grew a formalistic and legalistic decision-tree that first and foremost cared who a person's employer was, rather than what that person did. Since 1962, some of the little gears of the greater federal machine have adapted, creating reams and reams of regulations all trying, and largely failing, to mimic in some form at least part of the protection a single paragraph had provided for ninety-nine years.

Reinvigorating this part of our jurisprudence would create a single standard, jettisoning unnecessary and immaterial questions of who works for who and how. From that single standard, we may decide to hold government employees to a higher standard, as 18 U.S.C. § 208 does. And from that single standard, the law can finally be harmonized. Procurement regulations could build from a single law, implementing it for the particulars relevant to its needs. Grant regulations could do the same. And OTAs would actually have something prohibiting conflicted public acquisition by private individuals.

How that law reads and what it should specifically say is a question for another day. This article has advocated for a generally applicable criminal law prohibiting conflicted public acquisition. History through the present day provides many examples to build from—from the original Civil War statute and its iterations to the 1962 government employee-only law of today; from the earliest regulatory attempts to control what Congress unleashed in 1962 to today's FAR Subpart 3.11 policy statements. Those and more are catalogued in the appendix giving potential drafters a place to start.

Hopefully, this article has demonstrated why those drafters should get busy.

---

audit wherein a prime contractor under $5M did not flow down certain organizational conflict of interest clauses). Why no one realized that organizational conflict of interest is not a federal crime, and thus is irrelevant to FAR Subpart 3.10, is unknown.

**Figure 1**: Legal Controls Concerning Conflicts of Interest and Use of Non-Public Information for Personal Gain Applicable to Government Acquisition Professionals

| **A. Authority** | **B. Conflict of Interest Control** | **C. Definition of "Conflict of Interest"** | **D. Control on Use of Non-Public Information** | **E. Definition of "Non-Public Information"** | **F. To which Government Employees do the Controls Apply** |
|---|---|---|---|---|---|
| 1. 18 U.S.C. § 208(a) | Participation "personally and substantially . . . through decision, approval, disapproval, recommendation, the rendering of advice, investigation, or otherwise, in a . . . particular matter in which, to his knowledge, he, his spouse, minor child, [and certain organizations affiliated with the employee] has a financial interest[.]"[1] | No statutory definitions but OGE, in consultation with the Attorney General, empowered to exempt certain financial interests as "too remote or too inconsequential to affect the integrity of the services"[2] and "provide guidance with respect to the types of interests that are not so substantial as to be deemed likely to affect the integrity of the services."[3] | None. | None. | "[W]hoever, being an officer or employee of the executive branch of the United States Government, or of any independent agency of the United States, a Federal Reserve bank director, officer, or employee, or an officer or employee of the District of Columbia, including a special Government employee[.]"[4] |

[1] 18 U.S.C. § 208(a) (2013).

[2] 18 U.S.C. § 208(b)(2) (2013).

[3] 18 U.S.C. § 208(d)(2) (2013).

[4] 18 U.S.C. § 208(a) (2013).

| A. Authority | B. Conflict of Interest Control | C. Definition of "Conflict of Interest" | D. Control on Use of Non-Public Information | E. Definition of "Non-Public Information" | F. To which Government Employees do the Controls Apply |
|---|---|---|---|---|---|
| 2. 17 C.F.R. § 240.10b -5 | None. | None. | Prohibits insider trading under "classical"[5] and "misappropriation" theory.[6] | Information the person has a duty not to disclose.[7] | Applies to security[8] transactions by an insider or one who owes a duty of nondisclosure to the source of the inside information.[9] |

[5] U.S. v. O'Hagan, 521 U.S. 642, 651-2 (1997) ("Under the 'traditional . . . theory' of insider trading liability, [15 U.S.C. § 78j] and [17 C.F.R. § 240.10b-5] are violated when a corporate insider trades in the securities of his corporation on the basis of material, non-public information. Trading on such information qualifies as a deceptive device under [15 U.S.C. § 78j], we have affirmed, because a relationship of trust and confidence [exists] between the shareholders of a corporation and those insiders who have obtained confidential information by reason of their position with that corporation. . . .") (quotations omitted).

[6] *Id* at 652 ("The 'misappropriation theory' holds that a person commits fraud in connection with a securities transaction, and thereby violates [15 U.S.C. § 78j] and [17 C.F.R. § 240.10b-5], when he misappropriates confidential information for securities trading purposes, in breach of a duty owed to the source of the information. Under this theory, a fiduciary's undisclosed, self-serving use of a principal's information to purchase or sell securities, in breach of a duty of loyalty and confidentiality, defrauds the principal of the exclusive use of that information. In lieu of premising liability on a fiduciary relationship between company insider and purchaser or seller of the company's stock, the misappropriation theory premises liability on a fiduciary-turned-trader's deception of those who entrusted him with access to confidential information.") (quotations omitted).

[7] *See* 17 C.F.R. § 240.10b5-2 (2013) (providing operative definitions).

[8] *See* 15 U.S.C. § 78c (2013) (defining security).

[9] *O'Hagan* at 652-3 ("[T]he misappropriation theory outlaws trading on the basis of non-public information by a corporate 'outsider' in breach of a duty owed not to a trading party, but to the source of the information. The misappropriation theory is thus designed to 'protec[t] the integrity of the securities markets against abuses by 'outsiders' to a corporation who have access to confidential information that will affect th[e] corporation's security price when revealed, but who owe no fiduciary or other duty to that corporation's shareholders.'") (citations omitted).

| A. Authority | B. Conflict of Interest Control | C. Definition of "Conflict of Interest" | D. Control on Use of Non-Public Information | E. Definition of "Non-Public Information" | F. To which Government Employees do the Controls Apply |
|---|---|---|---|---|---|
| 3. Office of Gov't Ethics | Participation "personally and substantially in an official capacity in any particular matter in which, to his knowledge, he or any person whose interests are imputed to him under this statute has a financial interest, if the particular matter will have a direct and predictable effect on that interest."[10] | Prohibition self-defining.[11] | Shall "not engage in a financial transaction using non-public information, nor allow the improper use of non-public information to further his own private interest or that of another, whether through advice or recommendation, or by knowing unauthorized disclosure."[12] | "[I]nformation that the employee gains by reason of Federal employment and that he knows or reasonably should know has not been made available to the general public."[13] | "[O]fficer[s] or employee[s] of an agency, including a special Government employee [and] officers but not enlisted members of the uniformed services."[14] |

[10] 5 C.F.R. § 2635.402(a) (2013). The regulation purports to simply restate the statutory prohibition found at 18 U.S.C. § 208(a); however, the regulation includes a fourth element not mentioned in the statute: resolution of the "particular matter" must have a "direct and predictable effect on that interest." *See* U.S. v. Stadd, 636 F.3d 630, 639-40 (D.C. Cir. 2011) (sidestepping question of whether "direct and predictable effect" is an actual element of 18 U.S.C. § 208(a) by holding if it was error, such error was harmless). *See also* 18 U.S.C. § 208(b)(2) (2013) (empowering the OGE to exempt from the statutory prohibition "financial interest[s] . . . too remote or too inconsequential to affect the integrity of the services . . . .").

[11] *See* 5 C.F.R. § 2635.402(b) (2013) for definitions of specific terms.

[12] 5 C.F.R. § 2635.703(a) (2013).

[13] 5 C.F.R. § 2635.703(b) (2013).

[14] 5 C.F.R. § 2635.102(h) (2013). *But see* U.S. DEP'T OF DEF., 5500.07-R, JOINT ETHICS REG. § 1-300b (30 Aug. 1993) (C7, 17 Nov. 2011) *available at* http://www.dtic.mil/whs/directives/corres/pdf/550007r.pdf (applying supplemental standards of ethical conduct to enlisted military members).

| A. Authority | B. Conflict of Interest Control | C. Definition of "Conflict of Interest" | D. Control on Use of Non-Public Information | E. Definition of "Non-Public Information" | F. To which Government Employees do the Controls Apply |
|---|---|---|---|---|---|
| 4. U.S. Courts | Conflicts of interest should be avoided.[15] | "[H]e or she (or the spouse, minor child residing in the judicial employee's household, or other close relative of the judicial employee) might be so personally or financially affected by a matter that a reasonable person with knowledge of the relevant facts would question the judicial employee's ability properly to perform official duties in an impartial manner."[16] | Prohibited from employing "confidential information" for "personal gain."[17] | None. | "[A]ll employees of the judicial branch except Justices; judges; and employees of the United States Supreme Court, the Administrative Office of the United States Courts, the Federal Judicial Center, the Sentencing Commission, and federal public defender offices."[18] |

[15] U.S. Courts, Guide to Judiciary Policy, Code of Conduct For Judicial Employees, Vol. 2, Part A, Chapter 3, Canon 3(F)(1), *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/conduct/Vol02A-Ch03.pdf. Additional conflict of interest controls exist. *See Id*. at Canon 3(F)(2).

[16] *Id. See also Id.* at Canon 3(F)(4) (additional rules defining a "financial interest").

[17] *Id.* at Canon 3(D).

[18] *Id.* at 310.10(a).

| A. Authority | B. Conflict of Interest Control | C. Definition of "Conflict of Interest" | D. Control on Use of Non-Public Information | E. Definition of "Non-Public Information" | F. To which Government Employees do the Controls Apply |
|---|---|---|---|---|---|
| 5. Cong. | None.[19] | None. | "[M]ay not use non-public information derived from such person's position as a Member of Congress or employee of Congress or gained from the performance of such person's official responsibilities as a means for making a private profit."[20] | None. | Members and employees of Congress.[21] |

[19] Both the Senate and House have guidance regarding conflicts of interest in their respective ethics publications. *See, e.g.,* U.S. SENATE SELECT COMMITTEE ON ETHICS, THE SENATE CODE OF OFFICIAL CONDUCT, 110th Cong. (2008), *available at* http://www.ethics.senate.gov/public/index.cfm/files/serve?File_id=efa7bf74-4a50-46a5-bb6f-b8d26b9755bf, HOUSE OF REPRESENTATIVES COMMITTEE ON STANDARDS OF OFFICIAL CONDUCT, HOUSE ETHICS MANUAL, 110th Cong. (2008 ed.), *available at* http://ethics.house.gov/sites/ethics.house.gov/files/documents/2008_House_Ethics_Manual.pdf, U.S. HOUSE OF REPRESENTATIVES, COMMITTEE ON ETHICS, RULES REGARDING PERSONAL FINANCIAL TRANSACTIONS (Nov. 29, 2011), *available at* http://ethics.house.gov/sites/ethics.house.gov/files/fin%20trans%20pink%20sheet.pdf.

[20] Stop Trading on Congressional Knowledge Act of 2012, Pub. L. No. 112-105, § 3, 126 Stat. 291, 292 (2012).

[21] *See* Stop Trading on Congressional Knowledge Act at § 3.

**Figure 2**: Legal Controls Concerning Conflicts of Interest and Use of Non-Public Information for Personal Gain Applicable to Contractor Acquisition Professionals

| **A. Authority** | **B. Conflict of Interest Control** | **C. Definition of "Conflict of Interest"** | **D. Control on Use of Non-Public Information** | **E. Definition of "Non-Public Information"** | **F. To which Contractor Employees do the Controls Apply** |
|---|---|---|---|---|---|
| 1. 17 C.F.R. § 240.10b-5[22] | None. | None. | Prohibits insider trading under "classical" and "misappropriation" theory. | Information the person has a duty not to disclose. | Applies to security transactions by an insider or one who owes a duty of nondisclosure to the source of the inside information. |

[22] For citations relevant to this entry, *see infra* Figure 1, Row 2.

| **A.**<br>**Authority** | **B.**<br>**Conflict of Interest Control** | **C.**<br>**Definition of "Conflict of Interest"** | **D.**<br>**Control on Use of Non-Public Information** | **E.**<br>**Definition of "Non-Public Information"** | **F.**<br>**To which Contractor Employees do the Controls Apply** |
|---|---|---|---|---|---|
| 2. Federal Acquisition Regulation [23] | "The Contractor shall - (1) Have procedures in place to screen covered employees for potential personal conflicts of interest [and] [p]revent personal conflicts of interest[.]"[24] | "'Personal conflict of interest' means a situation in which a covered employee has a financial interest, personal activity, or relationship that could impair the employee's ability to act impartially and in the best interest of the Government when performing under the contract."[25] | Contractors shall "Prohibit use of non-public information accessed through performance of a Government contract for personal gain[.]"[26] | "[A]ny Government or third-party information that (1) Is exempt from disclosure under the Freedom of Information Act (5 U.S.C. § 552) or otherwise protected from disclosure by statute, Executive order, or regulation; or (2) Has not been disseminated to the general public and the Government has not yet determined whether the information can or will be made available to the public."[27] | Employees or self-employed subcontractors preforming an acquisition function closely associated with inherently governmental functions.[28] |

[23] The FAR applies to executive agencies. *See* 41 U.S.C. § 133 (2013) (stating that the following organizations are subject to the FAR: the "Executive departments" of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, Interior, Justice, Labor, State, Transportation, Treasury, Veterans Affairs, *see* 5 U.S.C. § 101 (2013); the "Military departments"—Air Force, Army, and Navy, *see* 5 U.S.C. § 102 (2013); "an establishment in the executive branch (other than the United States Postal Service or the Postal Regulatory Commission) which is not an Executive department, military department, Government corporation, or part thereof, or part of an independent establishment," 5 U.S.C. § 104(1) (2013); and, "wholly owned Government corporation[s]" of the Commodity Credit Corporation, Community Development Financial Institutions Fund, Export-Import Bank of the United States, Federal Crop Insurance Corporation, Federal Prison Industries, Corporation for National and Community Service, Government National Mortgage Association, Overseas Private

Investment Corporation, Pennsylvania Avenue Development Corporation, Pension Benefit Guaranty Corporation, Saint Lawrence Seaway Development Corporation, Secretary of Housing and Urban Development when carrying out duties and powers related to the Federal Housing Administration Fund, Tennessee Valley Authority, Panama Canal Commission, Millennium Challenge Corporation, and the International Clean Energy Foundation, 31 U.S.C. 9101(3) (2013). *But see* Dep't of Transportation and Related Agencies Appropriations Act, Pub. L. No. 104-50, § 348, 109 Stat. 436, 460-1 (1995) (codified at 49 U.S.C. § 40110(d)) (allowing the Federal Aviation Administration, a part of the Department of Transportation, to establish its own procurement regulation separate and apart from the FAR).

[24] FAR 52.203-16(b) (2013). *See also* Duncan Hunter National Defense Authorization Act for Fiscal Year 2009, Pub. L. No. 110-417, § 841, 122 Stat. 4356, 4537-9 (2008) (the progenitor of FAR Subpart 3.11), Preventing Personal Conflicts of Interest for Contractor Employees Performing Acquisition Functions, 76 Fed. Reg. 68,017 (Nov. 2, 2011) (final rule).

[25] FAR 52.203-16(a) (2013). The definition also states "[a] de minimis interest that would not 'impair the employee's ability to act impartially and in the best interest of the Government' is not covered under this definition. (1) Among the sources of personal conflicts of interest are—(i) Financial interests of the covered employee, of close family members, or of other members of the covered employee's household; (ii) Other employment or financial relationships (including seeking or negotiating for prospective employment or business); and (iii) Gifts, including travel. (2) For example, financial interests referred to in paragraph (1) of this definition may arise from—(i) Compensation, including wages, salaries, commissions, professional fees, or fees for business referrals; (ii) Consulting relationships (including commercial and professional consulting and service arrangements, scientific and technical advisory board memberships, or serving as an expert witness in litigation); (iii) Services provided in exchange for honorariums or travel expense reimbursements; (iv) Research funding or other forms of research support; (v) Investment in the form of stock or bond ownership or partnership interest (excluding diversified mutual fund investments); (vi) Real estate investments; (vii) Patents, copyrights, and other intellectual property interests; or (viii) Business ownership and investment interests." *Id.*

[26] FAR 52.203-16(b)(2)(ii) (2013).

[27] FAR 52.203-16(a) (2013).

[28] *See* FAR 3.1106 (2013). "Acquisition function closely associated with inherently governmental functions means supporting or providing advice or recommendations with regard to the following activities of a Federal agency: (1) Planning acquisitions[,] (2) Determining what supplies or services are to be acquired by the Government, including developing statements of work[,] (3) Developing or approving any contractual documents, to include documents defining requirements, incentive plans, and evaluation criteria[,] (4) Evaluating contract proposals[,] (5) Awarding Government contracts[,] (6) Administering contracts (including ordering changes or giving technical direction in contract performance or contract quantities, evaluating contractor performance, and accepting or rejecting contractor products or services)[,] (7) Terminating contracts[,] (8) Determining whether contract costs are reasonable, allocable, and allowable." FAR 52.203-16(a) (2013).

| **A.**<br>**Authority** | **B.**<br>**Conflict of Interest Control** | **C.**<br>**Definition of "Conflict of Interest"** | **D.**<br>**Control on Use of Non-Public Information** | **E.**<br>**Definition of "Non-Public Information"** | **F.**<br>**To which Contractor Employees do the Controls Apply** |
|---|---|---|---|---|---|
| 3. Council on Environmental Quality | Contractors developing environmental impact statements "shall execute a disclosure statement prepared by the lead agency, or where appropriate the cooperating agency, specifying that they have no financial or other interest in the outcome of the project."[29] | The contractor has "pecuniary or other interests in the outcomes of the [environmental impact statement]."[30] | None. | None. | Contractors creating environmental impact statements on behalf of a federal agency.[31] |

[29] 40 C.F.R. § 1506.5(c) (2013). *See* Implementation of Procedural Provisions, 43 Fed. Reg. 55,978; 55,987; 56,001 (Nov. 29, 1978).

[30] Guidance Regarding NEPA Regulations, 48 Fed. Reg. 34,263; 34,266 (July 28, 1983). *See also* Forty Most Asked Questions Concerning CEQ's National Environmental Policy Act Regulations, 46 Fed. Reg. 18,026, 18,031 (Mar. 23, 1981) (questions 17a and 17b concern conflicts of interest).

[31] *See* 40 C.F.R. § 1506.5(c) (2013). While the regulation likely meant "contractors" in the sense of a going business concern rather than its individual employees, the text could allow an agency to impute the conflicts of its employees to the contractor. This might be especially appropriate if the contractor is small or has a specific, dedicated team performing the contract.

| A. Authority | B. Conflict of Interest Control | C. Definition of "Conflict of Interest" | D. Control on Use of Non-Public Information | E. Definition of "Non-Public Information" | F. To which Contractor Employees do the Controls Apply |
|---|---|---|---|---|---|
| 4. Dep't. of Health & Human Services | Requiring institutions receiving Public Health Service (PHS) funding to "determine whether any significant financial interests relate to PHS–funded research; determine whether a financial conflict of interest exists; and, if so, develop and implement a management plan that shall specify the actions that have been, and shall be, taken to manage such financial conflict of interest."[32] | "[A] significant financial interest that could directly and significantly affect the design, conduct, or reporting of [Public Health Service] funded research."[33] | None. | None. | An "Investigator" who is "the project director or principal Investigator and any other person, regardless of title or position, who is responsible for the design, conduct, or reporting of research funded by the PHS, or proposed for such funding, which may include, for example, collaborators or consultants."[34] |

[32] 45 C.F.R. § 94.5(a) (2013). *See* Objectivity in Research, 60 Fed. Reg. 35,810, 35,818 (July 11, 1995) (final rule).

[33] 45 C.F.R. § 94.3 (2013). The regulation contains a lengthy definition of the term "significant financial interest." *Id.* Generally, the term means receipt of over $5,000 during the past twelve months from a private or publicly traded company; possession of an ownership interest in a publically traded company exceeding $5,000; possession of any ownership interest in a private company; and, possession of any related intellectual property rights, by the by the Investigator, the Investigator's spouse, or the Investigator's dependent children. *Id.*

[34] 45 C.F.R. § 94.3 (2013).

| **A.**<br>**Authority** | **B.**<br>**Conflict of Interest Control** | **C.**<br>**Definition of "Conflict of Interest"** | **D.**<br>**Control on Use of Non-Public Information** | **E.**<br>**Definition of "Non-Public Information"** | **F.**<br>**To which Contractor Employees do the Controls Apply** |
|---|---|---|---|---|---|
| 5.<br>Dep't. of Energy | "[S]hall not be permitted to make or influence any decisions on behalf of the contractor which directly or indirectly affect the interest of the Government, if the employee's personal concern in the matter may be incompatible with the interest of the Government."[35] | None. | "Management and operating contractor employees shall not use privileged information for personal gain, or make other improper use of privileged information which is acquired in connection with their employment on contract work."[36] | None. | Employees of a management and operating contractor.[37] |

[35] DEARS 970.0371-6(a) (2013). *See* Rewrite of Regulations Governing Management and Operating Contracts, 65 Fed. Reg. 80,994, 81,012 (Dec. 22, 2000) (final rule). Contractor employees also "shall not, under circumstances which might reasonably be interpreted as an attempt to influence the recipients in the conduct of their duties, accept any gratuity or special favor from individuals or organizations with whom the contractor is doing business, or proposing to do business, in accomplishing the work under the contract." DEARS 970.0371-6(a) (2013). Such employees also may not take outside employment that will "[a]ppear to create a conflict-of-interest situation." DEARS 970.0371-7(b) (2013).

[36] DEARS 970.0371-5 (2013).

[37] *See supra* notes 35 and 36.

| A. Authority | B. Conflict of Interest Control | C. Definition of "Conflict of Interest" | D. Control on Use of Non-Public Information | E. Definition of "Non-Public Information" | F. To which Contractor Employees do the Controls Apply |
|---|---|---|---|---|---|
| 6. Federal Deposit Insurance Corp. (FDIC) | Shall "avoid a conflict of interest [and] be ethically responsible[.]"[38] | "(1) Has a personal, business, or financial interest or relationship that relates to the services you perform under the contract; (2) Is a party to litigation against [the FDIC], or represents a party that is; (3) Submits an offer to acquire an asset from [the FDIC] for which services were performed during the past three years, unless the contract allows for the acquisition; or (4) Engages in an activity that would cause [the FDIC] to question the integrity of the service you provided, are providing or offer to provide [the FDIC], or impairs your independence."[39] | "Neither you nor any person who performs services on your behalf may use . . . information obtained from [the FDIC] or a third party in connection with an FDIC contract[.]"[40] | None.[41] | All employees who "perform[], directly or indirectly, contractual services or functions on" the FDIC's behalf.[42] |

[38] 12 C.F.R. § 366.9 (2013). *See also* Minimum Standards of Integrity and Fitness for an FDIC Contractor, 67 Fed. Reg. 69,990, 69,992-3 (Nov. 20, 2002).

[39] 2 C.F.R. § 366.10 (2013).

[40] 12 C.F.R. § 366.13(a) (2013).

[41] The regulations provide two, non-inclusive, examples of inappropriate use of confidential information. Both examples concern the disclosure of information to a third party. Neither example concerns a contract employee's use of the information for personal gain. *See* 12 C.F.R. § 366.13(b) (2013).

[42] 12 C.F.R. 366.0(c) (2013).

| A. Authority | B. Conflict of Interest Control | C. Definition of "Conflict of Interest" | D. Control on Use of Non-Public Information | E. Definition of "Non-Public Information" | F. To which Contractor Employees do the Controls Apply |
|---|---|---|---|---|---|
| 7. Def., Dep't. of—Federally Funded Research & Development Center (FFDRC) | "Work performed . . . shall be characterized by a need for unquestioned objectivity, divorced from all conflicting interests, financial and commercial. This includes . . . personal conflicts of interest of employees[.]"[43] | "[P]ersonal activities, relationships, or financial interests" including "gifts [and] outside activities" that may cause the employee to "lack objectivity or be perceived to potentially lack objectivity[.]"[44] | FFRDC must have "policies and procedures to protect proprietary, privileged, and sensitive information from disclosure."[45] | None. | FFRDC employees "in a position to materially influence research findings and/or recommendations."[46] |

[43] *See* Memorandum from The Under Secretary of Defense to the Service Secretaries et al., subject: Federally Funded Research and Development Center (FFRDC) Avoidance of Conflict of Interest (26 Jan. 2007), *available at* http://www.dod.mil/pubs/foi/logistics_material_readiness/acq_bud_fin/10-F-0034Conflict_of_InterestPolicies&Procedures_to_be_Included_in_FFRDC_Sponsoring_Agreements.pdf.

[44] *Id.*

[45] *Id.*

[46] *Id.*

| A. Authority | B. Conflict of Interest Control | C. Definition of "Conflict of Interest" | D. Control on Use of Non-Public Information | E. Definition of "Non-Public Information" | F. To which Contractor Employees do the Controls Apply |
|---|---|---|---|---|---|
| 8. Def., Dep't. of— Source Selection | "[A]ctual or potential conflict of interest issues are resolved prior to granting access to any source selection information."[47] | Only a reference stating "(See CFR 2635)."[48] | Non-disclosure agreement.[49] | None. | Members of a source selection team.[50] |

[47] Memorandum from the Director, Defense Procurement and Acquisition Policy, Office of The Under Secretary of Defense to Military Services' Acquisition Personnel, subject: Department of Defense Source Selection Procedures para 1.4.1.2.6 (4 Mar. 2011), *available a*t http://www.acq.osd.mil/dpap/policy/policyvault/USA007183-10-DPAP.pdf.

[48] *Id*.

[49] *Id*.

[50] *Id*.

| A. Authority | B. Conflict of Interest Control | C. Definition of "Conflict of Interest" | D. Control on Use of Non-Public Information | E. Definition of "Non-Public Information" | F. To which Contractor Employees do the Controls Apply |
|---|---|---|---|---|---|
| 9. Dep't. of the Air Force | Must report "real, apparent, possible, or potential conflict of interest[s]" and submit a "Conflict of Interest Statement . . . to the Contracting Officer indicating my personal stock holdings prior to accessing source selection information."[51] | None. | "I do solemnly swear or affirm that I will not divulge, publish, or reveal by word, conduct, or any other means," source selection or proprietary information."[52] | Non-disclosure obligation only applies to source selection[53] and proprietary information. | Members of a source selection team.[54] |

[51] Policy Memo 11-C-04, Acting Deputy Assistant Secretary (Contracting), subject: Mandatory Air Force Source Selection Procedure (8 May 2011), *available at* http://ww3.safaq.hq.af.mil/shared/media/document/AFD-110511-038.pdf [hereinafter SAF/AQC, *Source Selection Procedures*]. Contractor employees participating in the source selection must also certify "that neither I nor my immediate family, to the best of my knowledge, possess any financial interest" in any offeror exceeding $15,000. *Id*. at 16.

[52] *Id.* at 15.

[53] *See* 41 U.S.C. § 2101(7) (2013) (defining source selection information under the Procurement Integrity Act as "any of the following information prepared for use by a Federal agency to evaluate a bid or proposal to enter into a Federal agency procurement contract, if that information previously has not been made available to the public or disclosed publicly: (A) Bid prices submitted in response to a Federal agency solicitation for sealed bids, or lists of those bid prices before public bid opening[;] (B) Proposed costs or prices submitted in response to a Federal agency solicitation, or lists of those proposed costs or prices[;] (C) Source selection plans[;] (D) Technical evaluation plans[;] (E) Technical evaluations of proposals[;] (F) Cost or price evaluations of proposals[;] (G) Competitive range determinations that identify proposals that have a reasonable chance of being selected for award of a contract[;] (H) Rankings of bids, proposals, or competitors[;] (I) Reports and evaluations of source selection panels, boards, or advisory councils[;] (J) Other information marked as "source selection information" . . . by the head of the agency, the head's designee, or the contracting officer . . . ."). *See also* FAR 2.101 (2013) (defining source selection information similarly).

[54] *See* SAF/AQC, *Source Selection Procedures, supra* note 51, at 22-3.

| A. Authority | B. Conflict of Interest Control | C. Definition of "Conflict of Interest" | D. Control on Use of Non-Public Information | E. Definition of "Non-Public Information" | F. To which Contractor Employees do the Controls Apply |
|---|---|---|---|---|---|
| 10. U.S. Agency for Int'l Develop-ment | "[C]ontractor employees or consultants shall not engage "directly or indirectly . . . in any business, profession or occupation in the Cooperating Country or other foreign countries to which he/she is assigned, nor shall he make loans or investments to or in any business, profession or occupation in the Cooperating Country or other foreign countries in which he/she is assigned."[55] | None. | None. | None. | All USAID services contracts involving performance overseas.[56] |

[55] 48 C.F.R § 752.7027(e) (2013). *See also* Physical Fitness and Medical Privileges, 56 Fed. Reg. 7,586, 7,587 (Feb. 25, 1991) (final rule).

[56] *See* 48 C.F.R. § 752.7027 (2013) (preamble to clause).

| A. Authority | B. Conflict of Interest Control | C. Definition of "Conflict of Interest" | D. Control on Use of Non-Public Information | E. Definition of "Non-Public Information" | F. To which Contractor Employees do the Controls Apply |
|---|---|---|---|---|---|
| 11. Environmental Protection Agency | Contractor must report "actual or potential personal conflict of interest[.]"[57] | A "relationship of an employee, subcontractor employee, or consultant with an entity that may impair the objectivity of the employee, subcontractor employee, or consultant in performing the contract work."[58] | May not disclose "confidential business information[.]"[59] | "[A]ny information which pertains to the interests of any business, which was developed or acquired by that business[.]"[60] | Conflict of interest controls apply to employees "working on or having access to information regarding this contract[.]"[61]<br><br>The disclosure of non-public information controls apply contractor employees providing "advisory services[.]"[62] |

[57] 48 C.F.R. § 1552.209-73(b) (2013). *See also* Acquisition Regulation Concerning Conflicts of Interest, 59 Fed. Reg. 18,600, 18,620 (Apr. 19, 1994) (final rule).

[58] 48 C.F.R. § 1552.209-73(b) (2013). *See also* Acquisition Regulation Concerning Conflicts of Interest at 18,610 ("The critical test that a contractor must use regarding any potential [personal] conflict is whether a conflict exists which would impair the person's objectivity in performing the work under an EPA contract.).

[59] 48 C.F.R. § 1509.505-4 (2013).

[60] 40 C.F.R. § 2.201(c) (2013). The Environmental Protection Agency has extensive regulations on disclosure of information, many relevant to contractor operations. *See generally* 40 C.F.R. Part 2, Public Information (2013).

[61] 48 C.F.R. § 1552.209-73(b) (2013).

[62] 48 C.F.R. § 1509.505-4 (2013).

| A. Authority | B. Conflict of Interest Control | C. Definition of "Conflict of Interest" | D. Control on Use of Non-Public Information | E. Definition of "Non-Public Information" | F. To which Contractor Employees do the Controls Apply |
|---|---|---|---|---|---|
| 12. Nuclear Regulatory Council (NRC) | NRC has a policy against non-competitive procurements with contractors employing certain former NRC employees.[63] | Policy pertains to former NRC employees separated from the NRC for less than two years.[64] | Any information protected from release by either the Privacy Act or Freedom of Information Act.[65] | As defined in the Privacy Act[66] and Freedom of Information Act.[67] | N/A |

[63] *See* 48 C.F.R. § 2009.100(a) (2013). *See* 48 C.F.R. § 2052.209-70 (2013) (implementing clause). *See also* Acquisition Regulation (NRCAR), 64 Fed. Reg. 49,322, 49,327 (Sept. 10, 1999) (final rule).

[64] *See* 48 C.F.R. § 2009.100(a) (2013).

[65] "(1) If, in the performance of this contract, the contractor obtains access to information, such as NRC plans, policies, reports, studies, financial plans, internal data protected by the Privacy Act of 1974 or the Freedom of Information Act, the contractor agrees not to: (i) Use this information for any private purpose until the information has been released to the public; (ii) Compete for work for the Commission based on the information for a period of six months after either the completion of this contract or the release of the information to the public, whichever is first; (iii) Submit an unsolicited proposal to the Government based on the information until one year after the release of the information to the public; or (iv) Release the information without prior written approval by the contracting officer unless the information has previously been released to the public by the NRC. (2) In addition, the contractor agrees that, to the extent it receives or is given access to proprietary data, data protected by the Privacy Act of 1974 or the Freedom of Information Act, or other confidential or privileged technical, business, or financial information under this contract, the contractor shall treat the information in accordance with restrictions placed on use of the information." 48 C.F.R. § 2052.209-72(e) (2013) (internal parentheticals omitted).

[66] *See* 5 U.S.C. § 552a (2013).

[67] *See* 5 U.S.C. § 552 (2013).

| A. Authority | B. Conflict of Interest Control | C. Definition of "Conflict of Interest" | D. Control on Use of Non-Public Information | E. Definition of "Non-Public Information" | F. To which Contractor Employees do the Controls Apply |
|---|---|---|---|---|---|
| 13. U.S. Courts[68] | No contractor employee may be an "officer or employee" of the federal government and no person with a financial interest in a privately owned contractor shall be an "officer or employee" of the federal government.[69]<br><br>"No employee, principal, or affiliate" may have a conflict of interest.[70] | A spouse, child, or parent's ownership interest in the contractor will be imputed to the person.[71] | Will not disclose any information "received or generated under the contract[.]"[72] | None. | Conflict of interest controls apply to all employees of contractors providing services.[73]<br><br>Disclosure of non-public information controls apply to employees of contractors providing expert or consultant services.[74] |

[68] In addition to the controls listed here, the Code of Conduct for Judicial Employees can be applied to contractors. *See* U.S. COURTS, GUIDE, CODE OF CONDUCT FOR JUDICIAL EMPLOYEES, Vol. 2, Part A, § 310.10(d) (2013), *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/conduct/Vol02A-Ch03.pdf ("Contractors and other nonemployees who serve the judiciary are not covered by this code, but appointing authorities may impose these or similar ethical standards on such nonemployees, as appropriate.").

[69] UNITED STATES COURTS, GUIDE TO JUDICIARY POLICY, SOLICITATION PROVISIONS AND CONTRACT CLAUSES, Vol. 14; App. 1B, Clause 1-1 (2013), *available at* http://www.uscourts.gov/uscourts/FederalCourts/Procurement/Guide/Vol14-Ch01-Appx1B.pdf?page=1#page=1.

[70] *Id.* at App. 1B, Clause 1-5(a).

[71] *Id.* at App. 1B, Clause 1-1(d).

[72] *Id.* at App. 1B, Clause 5-5.

[73] *Id.* at App. 1B, Clause 1-5.

[74] *Id.* at Vol 14, Ch. 5, § 520.75.

| A. Authority | B. Conflict of Interest Control | C. Definition of "Conflict of Interest" | D. Control on Use of Non-Public Information | E. Definition of "Non-Public Information" | F. To which Contractor Employees do the Controls Apply |
|---|---|---|---|---|---|
| 14. Federal Aviation Agency | "[N]on-Federal" members of a "service organization" shall not have real or apparent conflicts of interest.[75] | Regulation adopts definitions found in 18 U.S.C. § 208 and 5 C.F.R. Part 2635. | None. | None. | Employees of a "service organization."[76] |

[75] FEDERAL AVIATION ADMINISTRATION, ACQUISITION MANAGEMENT POLICY (2008), ¶ 3.1.5; ¶ 4.2.3.14.4, *available at* http://fasteditapp.faa.gov/ams/do_action?do_action=ListTOC&contentUID=4.

[76] "A service organization is any organization that manages investment resources regardless of appropriation to deliver services. It may be a service unit, program office, or directorate, and may be engaged in air traffic services, safety, security, regulation, certification, operations, commercial space transportation, airport development, or administrative functions." *Id.* at App. C.

| A. Authority | B. Conflict of Interest Control | C. Definition of "Conflict of Interest" | D. Control on Use of Non-Public Information | E. Definition of "Non-Public Information" | F. To which Contractor Employees do the Controls Apply |
|---|---|---|---|---|---|
| 15. Troubled Assets Relief Program | Prohibits any "personal conflicts of interest[.]"[77] | "[M]eans a personal, business, or financial interest of an individual, his or her spouse or any dependent child that could adversely affect the individual's ability to perform under the arrangement, his or her objectivity or judgment in such performance, or his or her ability to represent the interests of the Treasury."[78] | Shall not "[u]se or allow the use of any non-public information to further any private interest[.]"[79] | "Any information that Treasury provides to a retained entity under an arrangement, or that the retained entity obtains or develops pursuant to the arrangement[.]"[80] | Conflict of interest controls apply to "key individuals."[81]<br><br>Use of non-public information controls apply to "retained entities."[82] |

[77] 31 C.F.R. § 31.212(a) (2013). *See also* TARP Conflicts of Interest, 76 Fed. Reg. 61,046, 61,050 (Oct. 3, 2011) (final rule).

[78] 31 C.F.R. § 31.201 (2013).

[79] 31 C.F.R. § 31.217(b)(2) (2013).

[80] 31 C.F.R. § 31.217(a) (2013).

[81] *See* 31 C.F.R. § 31.212(a) (2013). "Key individual means an individual providing services to a private sector entity who participates personally and substantially, through, for example, decision, approval, disapproval, recommendation, or the rendering of advice, in the negotiation or performance of, or monitoring for compliance under, the arrangement with the Treasury." 31 C.F.R. § 31.201 (2013).

[82] *See* 31 C.F.R. § 31.217(b)(2) (2013). "Retained entity means the individual or entity seeking an arrangement with the Treasury or having such an arrangement with the Treasury, but does not include special government employees. A 'retained entity' includes the subcontractors and consultants it hires to perform services under the arrangement." 31 C.F.R. § 31.201 (2013).

| A. Authority | B. Conflict of Interest Control | C. Definition of "Conflict of Interest" | D. Control on Use of Non-Public Information | E. Definition of "Non-Public Information" | F. To which Contractor Employees do the Controls Apply |
|---|---|---|---|---|---|
| 16. Information Tech. Exchange Program[83] | Assigned personnel "deemed" federal employee for "section[] 208 . . . of title 18"[84] | No statutory definitions but the Office of Government Ethics, in consultation with the Attorney General, empowered to exempt certain financial interests as "too remote or too inconsequential to affect the integrity of the services"[85] and "provide guidance with respect to the types of interests that are not so substantial as to be deemed likely to affect the integrity of the services."[86] | Assigned personnel "deemed" federal employee for "section[] 1905 . . . of title 18"[87] and "may not have access to any trade secrets or to any other non-public information which is of commercial value to the private sector organization from which he is assigned[.]"[88] | None. | Private sector employees assigned to agencies under the Information Technology Exchange Program. |

[83] The Information Technology Exchange Program existed for five years after Dec. 17, 2002. *See* 5 U.S.C. § 3701-7 (2013) (the program). *See also* E-Government Act of 2002, Pub. L. No. 107-347, § 209(c), 116 Stat. 2899, 2925-32 (2002) (establishing the program). In 2009, Congress provided the Secretary of Defense authority to conduct a very similar program, but no assignment could commence after Sept. 30, 2013. See National Defense Authorization Act for Fiscal Year 2010, Pub. L. No. 111-84, § 1110, 123 Stat. 2190, 2493-5 (2009).

[84] 5 U.S.C. § 3704(b)(2)(B) (2013).

[85] 18 U.S.C. § 208(b)(2) (2013).

[86] 18 U.S.C. § 208(d)(2) (2013).

[87] 5 U.S.C. § 3704(b)(2)(B) (2013).

[88] 5 U.S.C. § 3704(b)(3) (2013).

**Figure 3**: Legal Controls Concerning Conflicts of Interest and Use of Non-Public Information for Personal Gain Applicable to Grantee Acquisition Professionals

| **A. Authority** | **B. Conflict of Interest Control** | **C. Definition of "Conflict of Interest"** | **D. Control on Use of Non-Public Information** | **E. Definition of "Non-Public Information"** | **F. To which Grantee Employees do the Controls Apply** |
|---|---|---|---|---|---|
| 1. 17 C.F.R. § 240.10b-5[89] | None. | None. | Prohibits insider trading under "classical" and "misappropriation" theory. | Information the person has a duty not to disclose. | Applies to security transactions by an insider or one who owes a duty of nondisclosure to the source of the inside information. |

[89] For citations relevant to this entry, *see infra* Figure 1, Row 2.

| A. Authority | B. Conflict of Interest Control | C. Definition of "Conflict of Interest" | D. Control on Use of Non-Public Information | E. Definition of "Non-Public Information" | F. To which Grantee Employees do the Controls Apply |
|---|---|---|---|---|---|
| 2. Office of Management & Budget (OMB)[90] –Standard Forms for All Grant Applicants | The "duly authorized representative of the applicant" certifies the applying organization "[w]ill establish safeguards to prohibit employees from using their positions for a purpose that constitutes or presents the appearance of personal or organizational conflict of interest[.]"[91] | None. | The "duly authorized representative of the applicant" certifies the applying organization "Will establish safeguards to prohibit employees from using their positions for . . . personal gain."[92] | None. | All. |

[90] *See* 31 U.S.C. § 503(b)(2)(C) (2013) (The OMB "Deputy Director for Management shall establish general management policies for executive agencies and perform the following general management functions: . . . Perform all functions of the Director . . . relating to . . . grant, cooperative agreement, and assistance management . . . ."). The OMB promulgates grant regulations under two separate regimes: institutions of higher education, hospitals, and other non-profit organizations; and, state, local, and tribal governments. *Compare* 2 C.F.R. § 215.0 (2013) (stating grant regulations under Part 215 of the Title 2 of the Code of Federal Regulations applies to institutions of higher education, hospitals, and other non-profit organizations), *with* Office of Mgmt. & Budget, Exec. Office of the President, OMB Circular No. A-102 (Revised), Grants and Cooperative Agreements with State and Local Governments ¶ 1 (1997) (stating OMB Circular No. A-102 "establishes consistency and uniformity among Federal agencies in the management of grants and cooperative agreements with State, local, and federally-recognized Indian tribal governments.").

[91] Office of Mgmt. & Budget, Exec. Office of the President, Standard Forms 424B ¶ 3 & 424D ¶ 7, *available at* http://apply07.grants.gov/apply/FormLinks?family=15. *Compare* 2 C.F.R. § 215.12 (2013), *with* Office of Mgmt. & Budget, Exec. Office of the President, OMB Circular No. A-102 (Revised), Grants and Cooperative Agreements with State and Local Governments, attachment ¶ (1)(c)(1) (1997) (both sets of grant rules require agencies to use certain standard forms like SF-424B and SF-424D).

[92] *See supra* note 91.

| **A. Authority** | **B. Conflict of Interest Control** | **C. Definition of "Conflict of Interest"** | **D. Control on Use of Non-Public Information** | **E. Definition of "Non-Public Information"** | **F. To which Grantee Employees do the Controls Apply** |
|---|---|---|---|---|---|
| 3. OMB—Instit. of Higher Learning, Hospitals, or Other Non-Profit Grantees | "No employee, officer, or agent [of the grantee] shall participate in the selection, award, or administration of a contract supported by Federal [grant] funds if a real or apparent conflict of interest would be involved."[93] | "[W]hen the employee, officer, or agent, any member of his or her immediate family, his or her partner, or an organization which employs or is about to employ any of the parties indicated herein, has a financial or other interest in the firm selected for an award."[94] | None. | None. | Those participating in the "the selection, award, or administration of a contract supported by Federal [grant] funds[.]"[95] |
| 4. OMB—State, Local, and Tribal Govern-ments | None. | None. | None. | None. | None. |

[93] 2 C.F.R. § 215.42 (2013).

[94] *Id.*

[95] 2 C.F.R. § 215.42 (2013).

# BEYOND *SKYNET*: RECONCILING INCREASED AUTONOMY IN COMPUTER-BASED WEAPONS SYSTEMS WITH THE LAWS OF WAR

*Captain Christopher M. Kovach**



* Capt Christopher M. Kovach, Judge Advocate, United States Air Force (J.D., *cum laude*, University of Pittsburgh (2008); M.S., International Relations and National Security Studies, Troy University (2011); B.S., Information Sciences & Technology and French, Pennsylvania State University (2005)), is a Legal Advisor to the North American Aerospace Defense Command (NORAD), Continental U.S. Region, 601st Air and Space Operations Center, Tyndall Air Force Base (AFB), Florida. Previous assignments include Chief of Military Justice, Aeronautical Systems Center, Wright-Patterson AFB, Ohio; Contracts and Fiscal Law Attorney, Combined Joint Interagency Task Force 435, Kabul, Afghanistan; and Deputy Chief of Military Justice, Kadena Air Base, Japan. Member of the Bar of the State of Pennsylvania. The author thanks the following contributors: Colonel Michael Guillory, Florida Air National Guard; Lieutenant Colonel Neil H. Stallings, U.S. Air Force Reserves; Captain Rebekah Byrd, U.S. Air Force; and Mr. Edward Ropple for their insights and assistance in crafting this article.

Skynet *was a computer system developed for the U.S. military by the defense firm Cyberdyne Systems*. Skynet *was first built as a "Global Digital Defense Network" and given command over all computerized military hardware and systems, including the B-2 stealth bomber fleet and America's entire nuclear weapons arsenal. The strategy behind* Skynet's *creation was to remove the possibility of human error and slow reaction time to guarantee a fast, efficient response to enemy attack*.[1]

The preceding description is, as anyone conversant in American cinema knows, purely fiction. The computer system that gained self-awareness only to wreak havoc upon humanity lives inside the *Terminator* movie franchise. But the questions concerning the danger of pseudo-sentient computers raised by James Cameron's 1984 film nevertheless prove prescient today, where United States Department of Defense (DoD) regularly employs autonomous weapons systems. In a 2012 memorandum outlining policies concerning their use, the Deputy Secretary of Defense highlighted a desire to avoid unintended engagements and minimize the probability of their occurrence.[2] Otherwise stated, DoD seeks to avoid a "Skynet moment,"[3] where a preprogrammed weapon system inadvertently attacks an innocent target.[4]

---

[1] Referencing the purely fictional Skynet artificial intelligence network employed in the *Terminator* franchise, popularized by Arnold Schwarzenegger. *Skynet (Terminator)*, Wikipedia, http://en.wikipedia.org/wiki/Skynet_(Terminator) (last visited Jan. 2, 2013). This should not be confused with the wholly real array of military satellites, coincidentally named Skynet, launched by the United Kingdom. Jonathan Amos, *UK's Skynet Military Satellite Launched*, BBC News (Dec. 19, 2012), http://www.bbc.co.uk/news/science-environment-20781625.

[2] U.S. Dep't of Def., Dir. 3000.09, Autonomy in Weapons Systems para. 1(b) (21 Nov. 2012) [hereinafter DoD Dir. 3000.09], *available at* http://www.dtic.mil/whs/directives/corres/pdf/300009p.pdf (the directive "[e]stablishes guidelines designed to minimize the probability and consequences of failures in autonomous and semi-autonomous weapon systems that could lead to unintended engagements").

[3] The Deputy Assistant Secretary of Defense for Force Development made a similar allusion. Aaron Mehta, *U.S. DoD's Autonomous Weapons Directive Keeps Man in the Loop*, DefenseNews (Nov. 27, 2012), http://www.defensenews.com/article/20121127/DEFREG02/311270005/U-S-DoD-8217-s-Autonomous-Weapons-Directive-Keeps-Man-Loop ("'This directive is, for once, out ahead of events,' 'This isn't something where we all of a sudden realized someone's out there about to develop a *Terminator* and decided we better get a directive out. That's not the case.'").

[4] For instance, unmanned aerial vehicles like the MQ-1 Predator drone "can loiter over potential targets for hours before firing their missiles," making them incredibly versatile. *See, e.g.*, *Unmanned Aerial Vehicles: Death from Afar*, The Economist (Nov. 3, 2012), http://www.economist.com/news/international/21565614-america-uses-drones-lot-secret-and-largely-unencumbered-declared-rules-worries. No DoD proposal has suggested, or even hinted, automatically firing weapons—that is, a machine "pulling the trigger"—but the topic draws ample commentary. For instance, as *The Economist* pithily notes, "[b]omb-dropping remote-controlled planes will soon be commonplace. What if, by another country's reasonable lights, America's drone attacks count as terrorism? What if, according to the general principles implicitly governing the Obama administration's own drone campaign, 1600 Pennsylvania Avenue turns out to be a legitimate target for another country's drones? Were we to will Mr Obama's rules of engagement as universal law, *a la* Kant, would we find ourselves in harm's way? I suspect we would." *Obama's Drone Guidelines: Bombing Kant's Test*, The Economist (Nov. 30, 2012), http://www.economist.com/blogs/democracyinamerica/2012/11/obamas-drone-guidelines.

This policy, for whatever reason, fails to discuss the growing autonomy present in computer-based weapons systems, or "cyberweapons."[5] It also ignores their increasing prevalence.

For the purposes of this Article, "autonomous cyberweapons" are essentially computer-based variants of DoD's traditional definition of autonomous weaponry, which are weapons systems that:

> once activated, can select and engage targets without further intervention by a human operator. This includes human-supervised autonomous weapon systems that are designed to allow human operators to override operation of the weapon system, but can select and engage targets without further human input after activation.[6]

They might allow an end-user or operator to change some attack parameters and indeed override operations, but they possess decision-making algorithms crafted by programmers before the weapon's deployment. For these reasons, they differ from traditional semi-autonomous weapons, such as "fire and forget" weapons that rely upon technology to acquire, track, and engage human-selected targets because in those cases, "human control is retained over the decision to select individual targets and specific target groups for engagement."[7] In the case of autonomous cyberweapons, this human control is, at best, shared between the programmer and the operator; and in some cases, the operator might exercise almost no control whatsoever.[8]

At the outset, because the law of armed conflict (LOAC) applies only to recognized "attack," defining that level of belligerence is crucial. But no consensus definition exists, and other varieties of computer-based attacks might qualify instead, such as espionage, theft of intellectual property, or garden-variety criminal activity. The DoD definition of cyber-attack proves most useful, insofar as it codifies the views of the American government and ostensibly binds its military departments. In 2011, following the creation of the United States Cyber Command (USCYBERCOM), a

---

[5] This directive "[d]oes not apply to autonomous or semi-autonomous cyberspace systems for cyberspace operations; unarmed, unmanned platforms; unguided munitions; munitions manually guided by the operator (e.g., laser- or wire-guided munitions); mines; or unexploded explosive ordnance." DoD Dir. 3000.09, *supra* note 2, para. 2(a)(3)(b).

[6] DoD Dir. 3000.09, *supra* note 2, Part II.

[7] *Id*.

[8] Thus, unlike dumb bombs or pressure-activated land mines, autonomous cyberweapons boast decision-making algorithms that distinguish friend from foe and dictate how the weapon (often a piece of malware or malicious code that wreaks havoc on attached computers) moves through a network. The closest analogy might be computer-guided weaponry currently deployed aboard naval vessels and aircraft. These systems strike preselected targets when certain parameters are met. Autonomous cyberweapons do too, but could also possess the capacity to learn and adjust to dynamic battlefield conditions.

subordinate command[9] organized beneath United States Strategic Command, the lead agency for carrying out the American mission in cyberspace,[10] the Joint Chiefs of Staff adopted this definition:

> A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyber attack are not necessarily limited to the targeted computer systems or data themselves—for instance, attacks on computer systems which are intended to degrade or destroy infrastructure or [command and control] capability. A cyber attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber attack may be widely separated temporally and geographically from the delivery.[11]

Perhaps the most notable example of a successful attack delivered by an autonomous cyberweapon is "Stuxnet," a computer worm that infected Iranian industrial sites, damaging its uranium enrichment stations and dealing a real setback to Iran's nuclear ambitions. Some have remarked that the worm "accomplish[ed] what six years of United Nations Security Council resolutions could not."[12] No ordnance was dropped; no boots trampled through Tehran. Other memorable incidents include those on Estonia and Georgia in 2007 and 2008, and the emerging threat of a cyber-attack on U.S. critical infrastructure led the former Secretary of Defense,

---

[9] Technically, U.S. Cyber Command (USCYBERCOM) is a "subunified" command beneath U.S. Strategic Command (USSTRATCOM). Andrew Feickert, *The Unified Command Plan and Combatant Commands: Background and Issues for Congress*, Cong. Res. Service R42077 (Jan. 3, 2013), http://www.fas.org/sgp/crs/natsec/R42077.pdf. USSTRATCOM is a combatant command, of which the U.S. possesses nine: U.S. Africa Command (USAFRICOM); U.S. Central Command (USCENTCOM); U.S. European Command (USEUCOM); U.S. Northern Command (USNORTHCOM); U.S. Pacific Command (USPACOM); U.S. Special Operations Command (USSOCOM); U.S. Southern Command (USSOUTHCOM); U.S. Strategic Command (USSTRATCOM); U.S. Transportation Command (USTRANSCOM). Those focusing on geography have primary military authority in that region. The others, called functional combatant commands, span geographical lines entirely and focus upon special operations, transportation, and U.S. nuclear, space, and computer-based capabilities.

[10] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel, *The Law of Cyber-Attack*, 100 Calif. L. Rev. 817, 824 (2012) (noting that the laws of war apply only to the "small subset of cyber-attacks that do constitute armed attacks or that occur in the context of an ongoing armed conflict") [hereinafter The Law of Cyber-Attack].

[11] Memorandum from Gen. James E. Cartwright, to Chiefs of the Military Servs., Commanders of the Combatant Commands, Dirs. of the Joint Staff Directorates, subject: Joint Terminology for Cyberspace Operations 5 (Nov. 2011).

[12] Danielle Warner, *From Bombs and Bullets to Botnets and Bytes: Cyber War and the Need for a Federal Cybersecurity Agency*, 85 Calif. L. Rev. Postscript 1 (2012).

Leon Panetta, to warn of a "digital Pearl Harbor" in 2012.[13] More pointedly, unlike traditional munitions, weapons like Stuxnet boast a prolonged shelf life—Iran recently claimed that the virus again targeted one of its nuclear power plants after Stuxnet allegedly spread to computers in Indonesia, India, the United States, and elsewhere due to a programming bug.[14]

Closer to home, the day before DoD announced its policy regarding autonomous weapons systems, the Defense Advanced Research Projects Agency (DARPA) issued an announcement offering funding for its "Plan X" project, which aims to create an "end-to-end system that enables the military to understand, plan, and manage cyberwarfare in real-time, large-scale, and dynamic network environments."[15] Specifically, Plan X contemplates leveraging machine assistance to automate and simplify the cyberwarfare process.[16] It also aims to incorporate existing toolkits, such as the commercially available CANVAS framework to the freely available Metasploit system.[17] Once completed, the weapon could enable operators to "deploy attack libraries from a 'playbook' . . . [although] the code will be built with checks on what sorts of things it can do without human direction."[18] However, the software will usually operate independently, addressing DoD's principal complaint against manually operated cyber systems: that humans are too slow.[19]

---

[13] David Z. Bodenheimer, *Cyberwarfare in the Stuxnet Age: Can Cannonball Law Keep Pace with the Digital Battlefield?*, The SciTech Lawyer, vol. 8, no. 3 (Winter 2012), *available at* http://www.crowell.com/files/2012-bodenheimer-the-scitech-lawyer.pdf.

[14] Adrianne Jeffries, *Stuxnet Strikes Again, Iranian Official Says*, The Verge (Dec. 25, 2012), http://www.theverge.com/2012/12/25/3803216/stuxnet-strikes-again-iranian-official-says.

[15] Defense Advanced Research Projects Agency, *Broad Agency Announcement BAA-13-02: Foundational Cyberwarfare (Plan X)* (Nov. 20, 2012), https://www.fbo.gov/utils/view?id=49be462164f948384d455587f00abf19, at 8-9 [hereinafter DARPA Agency Announcement].

[16] *Id.* at 12.

[17] *Id.* at 17. These software programs are designed to provide their users with information concerning the target system's security vulnerabilities. *See, e.g.*, Tony Bradley, *Metasploit Framework: Walking the Thin Line Between a Tool and a Weapon*, Symantec.com, http://netsecurity.about.com/cs/hackertools/a/aa041004.htm (last visited Jan. 3, 2013); Pukhraj Singh and K.K. Mookhey, *Metasploit Framework*, Symantec.com (Nov. 2, 2010), http://www.symantec.com/connect/articles/metasploit-framework-part-1.

[18] Sean Gallagher, *U.S. Cyber Weapons Exempt from Human Judgment Requirement*, Ars Technica (Nov. 29, 2012), http://arstechnica.com/tech-policy/2012/11/us-cyber-weapons-exempt-from-human-judgment-requirement.

[19] "In essence, the current manual approach has defined the way cyber operations are conceived and would be conducted—as asynchronous actions. Manual processes provide no capacity for real-time assessment and adjustment to adapt to changing battlespace conditions. The current paradigm is a simple progression of plan, execute, plan, execute, plan, execute . . . however if the process can be technologically optimized and the time-intensive requirements minimized, commanders will be able to leverage cyber capabilities in a more flexible manner, consistent with kinetic capabilities, to achieve real-time, synchronous effects in the cyber battlespace." DARPA Agency Announcement, *supra* note 15, at 6.

Plan X, according to DARPA director Arati Prabhakar, simplifies the domain of cyberspace, with playbook attacks "as easy to launch as an Angry Bird."[20] At a demonstration in October 2012, a design firm vying for one of the program's contracts showcased the equivalent of a 40-inch iPad with the ability for multiple persons to operate it simultaneously, and another company, which previously worked on video games and G.I. Joe toys, proposed a game-like user interface that dazzled Pentagon officials and Capitol Hill staffers.[21]

This Article explores how LOAC applies to these autonomous cyberweapons, or software used to launch attacks in the domain of cyberspace. Part I examines whether the laws of war permit the deployment of autonomous cyberweapons. It begins by assessing how the principles of proportionality and distinction apply. Next, since LOAC prohibits any attack that might cause excessive collateral damage when compared to the military advantage gained, this section critically examines the important case of dual-use facilities, meaning the infrastructure jointly used by the military and civilians.[22] Finally, it concludes by exploring what mechanisms are needed to ensure these weapons respect the laws of war.

Part II analyzes the composition of non-uniformed DoD personnel in cyberweapons' design phases and how LOAC impacts their status as combatants. Civilians often participate in the design, creation, and maintenance of software, either as direct employees of the government employing them; as authors of software incorporated into larger, more capable cyberweapons; or as contractors hired to design a system that boasts offensive features. Involving non-uniformed personnel, such as civilians and contractors, in the design of autonomous cyberweapons could place them within the reach of LOAC for possible violations of the laws of war. This is problematic, as current DoD policy limits participation in cyber-attacks to uniformed military personnel. But how the Department conducts business could expose its civilians and contractors to criminal violations or the laws of war regardless of its stated policies.[23]

---

[20] Noah Schachtman, *This Pentagon Project Makes Cyberwar as Easy as Angry Birds*, Wired (May 28, 2013), http://www.wired.com/dangerroom/2013/05/pentagon-cyberwar-angry-birds/all/.

[21] *Id.*

[22] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol 1), art. 51(5)(b), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP1].

[23] One article incorrectly notes that National Guard members may not carry out cyber-attacks. The Law of Cyber-Attack, *supra* note 10, at 854 n. 151 ("The allocation of responsibilities for cyber-warfare has been examined by the U.S. armed forces—the recently declassified Air Force cyberspace operations document explains that National Guard members may train for, but not carry out, cyber-attacks."). The complexities of what status DoD personnel are currently operating under is certainly complex, but the governing Air Force regulation notes that National Guard or Air Guard members in Title 10, or federal status, may carry out cyber-attacks. U.S. Dep't. of Air Force, Air Force Doctrine Document 3-12, Cyberspace Planning (30 Nov. 2011) [hereinafter AFDD 3-12], *available at* http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-12.pdf. This is likely because, unless activated under federal status, a Guard member follows one chain of command, which flows from his state's governor.

Part III considers DoD's process for formally reviewing an autonomous cyberweapon's compliance with LOAC. With current guidance, there exists a real risk that legal advisors providing on-demand advice during a cyberweapon's operation knows little about the weapon or its capabilities. This invites collateral damage, and DoD can do better. Its attorneys must be technologically savvy, capable of asking pointed questions about its possible effects. This section explores the current legal review process for cyberweapons and identifies potential shortfalls.[24] It also offers suggestions for improving the process, grounded in the assumption that, while even the untrained can readily grasp the effects of most conventional weapons, cyberweapons are different. Moreover, the injection of autonomy and the interconnectedness of computer networks complicate their deployment. In response, DoD must stimulate the development and training of uniformed personnel, both to enhance cyberwarfare capabilities and to provide its operators with the knowledge and situational awareness to better ensure compliance with the laws of war.

Failing to adapt current processes to the idiosyncrasies of novel technologies risks triggering unintended engagements the United States seeks to avoid, as well as abrogating its duties under international law.[25] Any laxity in reviewing the impact of autonomous weapons also invites entirely plausible scenarios that could run afoul of LOAC, such as inadvertently shutting down hospital generators, residential power systems, or even overwhelming non-affiliated Internet Service Providers merely carrying traffic of all kinds.[26]

The connectedness of computer networks expanded significantly in recent decades: they support nations' defense, economic security, and public health efforts.[27]

---

[24] U.S. Dep't. of Air Force, Instr. 51-402, Legal Reviews of Weapons and Cyber Capabilities (27 July 2011) [hereinafter AFI 51-402], *available at* http://www.epublishing.af.mil/shared/media/epubs/AFI51-402.pdf.

[25] "In the study, development, acquisition or adoption of a new weapon, means or method of war, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party." AP1, *supra* note 22, art. 36. While the United States is not a party to this Protocol, because some argue that it might rise to the level of customary international law, it seems prudent. Pragmatically, it also reflects in-place DoD practices which might be better refined.

[26] Ellen Nakashima, *Obama Signs Secret Directive to Help Thwart Cyberattacks*, Wash. Post (Nov. 14, 2012), http://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html; Jakob Kellenberger, *International Humanitarian Law and New Weapon Technologies*, Int'l Comm. of the Red Cross (Aug. 8, 2011), http://www.icrc.org/eng/resources/documents/statement/new-weapon-technologies-statement-2011-09-08.htm.

[27] U.S. Government Accountability Office (as U.S. General Accounting Office), *Technology Assessment: Cybersecurity for Critical Infrastructure Protection*, GAO-04-321, at 18 (May 2004), *available at* http://www.gao.gov/new.items/d04321.pdf. As the GAO report attests, computer systems and networks were not exactly designed with security in mind, leaving them vulnerable. This report, to which the author contributed, was released in 2004. Things are not much better in 2013. Referencing the GAO's persistent but oft-ignored calls for action, one commentator notes

In the United States, these systems are so vital to the nation's continued operations that their "incapacity or destruction . . . would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[28] And these civilian-owned critical infrastructure sites assuredly occupy high-ranking slots on both defended asset lists and adversaries' target lists.[29]

One can certainly imagine that, in response to a threat from a hostile country, the United States could attempt to overwhelm and sanitize their networks—much like America strives to achieve dominance in the traditional domains of air, land, the seas, and space.[30] The equivalent of a "no-fly zone" in the cyberspace domain is readily conceivable. Moreover, given DoD's inherent mandate to defend against all attacks and the real possibility that autonomous cyberweapons could be employed against adversaries, adhering to the laws of war while developing this emergent domain will prove challenging.

The intersection of law and technology must resolve these issues. Rejecting this assertion, the former Deputy Judge Advocate General of the Air Force, Professor Charles J. Dunlap, Jr., suggests that untangling these factual complications rests solely within the domain of leadership, not of law:

---

that "[y]ears of recommendations from the Government Accountability Office and inspectors general have failed to significantly improve the country's cybersecurity posture at a time when the United States is becoming increasingly reliant on an interconnected information infrastructure." William Jackson, *U.S. Not Prepared for 'Potentially Devastating' Cyberattacks, House Panel Told*, GCN.COM (Mar. 17, 2011), http://gcn.com/GIG/gcn/Articles/2011/03/17/Critical-infrastructure-vulnerable-to-attack.aspx. *See also* Richard Chirgwin, *AusCERT 2012: Kaspersky Says Cyber-Attacks Could 'Take Us Back to the Pre-Electric Era'* CSO.COM (May 18, 2012), http://www.cso.com.au/article/424988/auscert_2012_kaspersky_says_cyber-attacks_could_take_us_back_pre-electric_era_/; *Critical U.S. Infrastructure Vulnerable to Cyber Attack, Congress Fails to Act*, PUBLIC BROADCASTING SYSTEM (Aug. 8, 2012), http://www.pbs.org/newshour/bb/science/july-dec12/cybersecurity_08-08.html.

[28] 42 U.S.C. § 5195c(e) (2006). The Homeland Security Act of 2002 incorporated this definition. Pub. L. No. 107-296, § 2, 116 Stat. 2135, 2140 (codified at 6 U.S.C. § 101(4) (2006)). For national defense purposes, a similar definition is also used. 50 U.S.C. app. §2152(2) (2006).

[29] *See*, *e.g.*, Daniel Fineren, *Energy Assets in Front Line of Cyber War*, REUTERS (May 31, 2012), http://www.reuters.com/article/2012/05/31/cyber-attacks-energy-idUSL5E8GT5AD20120531 ("Global energy infrastructure is more vulnerable than ever . . . . [b]ut the biggest threat to everything from power grids to digital oilfields may come from malware based on the Stuxnet worm, widely thought to have been sponsored by western government agencies, security experts say.").

[30] *See* JOINT CHIEFS OF STAFF, JOINT PUB. 3-0, JOINT OPERATIONS, at V-47 (Aug. 11, 2011) [hereinafter JP 3-0], *available at* http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf ("The cumulative effect of dominance in the air, land, maritime, and space domains and information environment (which includes cyberspace) that permits the conduct of joint operations without effective opposition or prohibitive interference is essential to joint force mission success. JFCs seek superiority in these domains to prepare the operational area and information environment and to accomplish the mission as rapidly as possible.").

> The ability (or inability) to determine facts is not a legal issue but a technical problem for the specialists to solve. [. . .] The same can be said for the legal requirement to assess the impact on civilians and civilian objects before launching a cyberattack. [. . .] Again, if the ability to make the calculations that political leaders and policymakers require as much as lawyers is inadequate, that is a technical, not a legal, issue.[31]

This is true, but law must still keep pace with technology. And in order for the law to be applied to the facts at hand, the underlying technology must be understood. Cyberspace is a new domain in warfare, but effects that shape the digital battlefield produce very real consequences. In the end, the complexities and interdependence of computer systems drag the question of collateral damage to the forefront more forcefully than ever before.

## I. APPLYING THE LAWS OF WAR TO AUTONOMOUS CYBERWEAPONS

At their most basic level, the laws of war[32] attempt to "restrict the aim of warfare to the achievement of military objectives."[33] Circumscribing the employment of certain weapons contributes to this objective. Under LOAC, the two fundamental principles governing weapon use are distinction and proportionality.[34] They apply regardless of the weapon type. In other words, software counts. But the condi-

---

[31] Stewart A. Baker and Charles J. Dunlap, Jr., *What Is the Role of Lawyers in Cyberspace?,* ABA Journal (May 1, 2012), http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare/. Major General Dunlap misses the mark: in order for lawyers to provide adequate counsel to their decision-making clients, a partnership which reduces the risk of non-compliance with LOAC, they must be equipped to work arm-in-arm with technical specialists. Otherwise stated, cyberweapons are not dumb bombs; an operator's keystroke—combined with autonomous programming—could produce potentially unknown or unanticipated effects.

[32] For the purposes of this Article, the laws of war, for simplification's sake, refer to *jus in bello* analyses concerning the legality of a cyber-attack. This Article does not address the question of what constitutes an 'armed attack' in violation of article 51 of the United Nations charter. Additionally, as one scholar notes, in recent literature the "terms 'armed conflict,' 'war,' and 'use of force' are used virtually interchangeably [and] the terms 'law of armed conflict,' 'law of war,' and 'international humanitarian law'" all refer to the same body of Geneva and Hague law that regulates the conduct of parties to an armed conflict by way of the principles of distinction, military necessity, proportionality, humanity, and chivalry." Davis Brown*, A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 Harv. Int'l L.J. 179, 181 n.14 (2006). For a comprehensive analysis of the interpretation of Articles 2(4) and 51 of the United Nations Charter, which restricts the use of force save in self-defense against an armed attack, *see* Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 Yale J. Int'l L. 421 (2011).

[33] Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 Lewis & Clark L. Rev. 1023, 1033 (2007).

[34] *See, e.g.*, Kenneth Anderson and Matthew Waxman*, Law and Ethics for Robot Soldiers*, Hoover Institution Policy Review no. 176 (Dec. 1, 2012), http://www.hoover.org/publications/policy-review/article/135336.

tions of cyberwarfare complicate *jus in bello* analyses, as an attack's result is not "immediately lethal or destructive and may only cause temporary incapacity of network systems."[35] These systems, often civilian-owned and operated, run trains, route air traffic, regulate telecommunications signals and the Internet, and provide the backbone for the operation of global financial markets.[36]

At the outset, giving targeting responsibility to computers raises preexisting concerns about the use of autonomous weapons systems altogether. Blending advances in automation with ideas drawn from science fiction, scholars anticipate that the future could easily bring preprogrammed sentry robots; drones that dynamically hunt prey; and even *Transformers*-like robots capable of assembling together to create a larger, more powerful weapon.[37] With them come a host of well-founded objections based upon international law[38] and even pragmatic concerns regarding the proliferation of robotic armies and the dehumanization of war.[39] When the Russian Deputy Prime Minister announces that Moscow envisions deploying robots capable of engaging terrorists without harming civilians, all while possessing the independence to evacuate injured soldiers, these concerns become more grounded in reality.[40]

Yet software is already autonomous—by definition it contains internal logic that must be followed, though at times it might pause to await user input. This autonomy will surely grow in the future, as weapons boast even more robust internal decision-making algorithms, like the kind destined for Plan X's playbooks. In these cases, the human element inheres in the designers' instructions. Much like smart bombs and cluster munitions, which boast the ability to detonate at a certain time, or a designated location, computer-based weapons systems rely upon the same,

---

[35] The Law of Cyber-Attack, *supra* note 10, at 850.

[36] Jonathan A. Ophardt, *Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield*, 9 Duke L. & Tech. Rev. 1, 2-3 (2010).

[37] Anderson & Waxman, *supra* note 34.

[38] *See, e.g.*, Human Rights Watch, Losing Humanity: The Case Against Killer Robots (Nov. 2012), *available at* http://www.hrw.org/sites/default/files/reports/arms1112ForUpload_0_0.pdf ("Fully autonomous weapons have the potential to increase harm to civilians during armed conflict. They would be unable to meet basic principles of international humanitarian law, they would undercut other, non-legal safeguards that protect civilians, and they would present obstacles to accountability for any casualties that occur.").

[39] Anderson & Waxman, *supra* note 34; *see also* Jonathan Y. Huang and Jarrod M. Rifkind, *The Challenges of Emerging Technologies to Human Assumptions in War Ethics*, Presentation at the Fort Leavenworth Ethics Symposium by the Command and General Staff College (Dec. 5, 2012), *available at* http://c.ymcdn.com/sites/www.leavenworthethicssymposium.org/resource/resmgr/2012_papers/huang_and_rifkind-challenges.pdf.

[40] Clay Dillow, *Russia Is Building Robots to 'Neutralize' Terrorists*, Popular Science (May 21, 2013), http://www.popsci.com/technology/article/2013-05/russia-building-robots-will-neutralize-terrorists.

but to a much more complicated degree, and this raises several questions under the traditional laws of war.

Despite the challenges posed by computer-based weaponry, the United States has codified its intent to follow international law in the domain of cyberspace.[41] And although the evolution of technology outpaces the law, actors marshaling the technology for the purposes of war must nevertheless assess what limits that circumscribe its use apply.[42] But these laws, designed to protect civilians on the battlefield, never formally contemplated protecting civilian information systems.[43] Thus, before delving into the principles of distinction and proportionality, the initial question worth exploring is whether LOAC even permits the use of autonomous cyberweapons like Stuxnet and similar programs, some of which attack and disable targeted computers or control systems with abandon.

### A. The Laws of War Prohibit Certain Autonomous Cyberweapons

The principle of distinction, codified in Articles 51(2) and 52(1) of Additional Protocol I of the Geneva Conventions of 1949, requires parties to conflicts to "distinguish between the civilian population and combatants."[44] Otherwise stated, it reflects an affirmative duty to minimize harm to noncombatants and their property.[45] Attacks unable to distinguish between these sets of persons are deemed indiscriminate and considered unlawful.[46] Conversely, to reduce confusion throughout the

---

[41] U.S. Dep't. of Defense, Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934 (Nov. 2011) [hereinafter DoD Cyberspace Policy Report], *available at* http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf. The United States' official position is that "[t]he law of war encompasses all international law for the conduct of hostilities binding on the United States or its individual citizens, including treaties and international agreements to which the United States is a party, and applicable customary international law." U.S. Dep't. of Def., Dir. 2311.03E, DoD Law of War Program, para. 3.1 (May 9, 2006), *available at* http://www.dtic.mil/whs/directives/corres/pdf/231101e.pdf.

[42] Hollis, *supra* note 33, at 1036 (noting that "the law of war governs [information operations] even without mentioning it specifically.") (citing AP1, *supra* note 22, art. 35.1 ("[T]he right of the Parties to the conflict to choose methods or means of warfare is not unlimited.")).

[43] The Law of Cyber-Attack, *supra* note 10, at 821 (noting that the laws of war apply only to the "small subset of cyber-attacks that do constitute armed attacks or that occur in the context of an ongoing armed conflict.").

[44] AP1, *supra* note 22, art. 48.

[45] "In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives." *Id.* art. 48.

[46] "The civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited." *Id.* art. 51(2). Similar protection extends to civilian-owned objects. "Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use

battlefield, LOAC also exerts a positive duty upon noncombatants to remain away from ongoing hostilities; otherwise they forfeit this aegis of protection.[47] However, responsibility for managing the employment of weapons remains with military commanders.[48]

Most LOAC inquiries concern a weapon's post-engagement use, such as whether combatants targeted protected groups or sites or the weapon resulted in unnecessary damage. For instance, they analyze whether a bomber pilot dropped ordnance upon a permissible target, or whether Marines in an urban firefight adequately assessed the risk of harming civilians before engaging their enemy. Responsibility for a weapon's use generally attaches to both its user and the military officer in command: the specific use, not the weapon itself, bears scrutiny. However, some weapons may be simply unable to tell targets apart despite the best efforts of the operator.[49] In these cases, the weapon itself is considered "inherently indiscriminate" and outright prohibited by the laws of war.[50]

Thus, autonomous cyberweapons that launch uncontrollable, indiscriminate attacks are prohibited by the laws of war. Broadly stated, every cyberweapon must be specifically engineered to respect these strictures. They must "possess the ability to be aimed, or to aim [themselves], at an acceptable legal level of discrimination."[51] Falling beneath that threshold of discrimination mandates a weapon's prohibition. In this regard, cyberweapons are no different than conventional weapons, few of which

---

make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage." *Id.* art. 52(2).

[47] Under LOAC, only lawful combatants may participate directly in hostilities, or else they lose their protected status. *Id*. art. 51(3).

[48] This was no easy task, even before the advent of cyberweapons. One U.S. Army colonel writes that:

> Modern technology demands an almost instantaneous consideration of military necessity, humanity, and chivalry. [A commander] must distinguish relevant from irrelevant targets, seeking only the destruction of legitimate objectives. He is expected to perform the Solomon-like task of proportioning the amount of military destruction with the military value of the objective. The voices of humanity remind a commander that war is a political weapon. Gratuitous unnecessary suffering or destruction is irrelevant to his military purpose and often counter-productive. Somehow he is to divine the least coercive method. Adding to the complexity, are the remnants of chivalry or professional courtesy which impose upon a representative of a proud military profession lineage and tradition which have their own imperatives.

William G. Eckhardt, *Command Criminal Responsibility: A Plea for a Workable Standard*, 97 Mil. L. Rev. 1, 3 (1982).

[49] Anderson & Waxman, *supra* note 34.

[50] *Id.*

[51] *Id.*

are banned, like poisonous, chemical, and biological weapons.[52] Although these weapons can be aimed by their operators, their effects are not fully controllable and therefore risk impacting large numbers of the civilian population indiscriminately.[53]

From the above provisos, this Article asserts two *ex-ante* conclusions: (1) directly attacking purely military computer systems, assuming absolutely zero risk of crossover into other networks is permissible, something likely unattainable in the real world; and (2) LOAC prohibits cyberweapons that indiscriminately attack all computer systems on a given network or connected networks. Viruses, or other forms of self-propagating malicious code, fall into this latter category. They assault all unprotected computers with abandon.[54] However, beyond this spectrum's two edge cases, the calculus becomes more complex, and most cyberweapons occupy a case between these endpoints.

B. Respecting the Principle of Distinction

To ensure cyberweapons operate within this permissible range, engineers could program them with fixed lists of permissible targets. Doing so places the weapon closer to the endpoint reserved for attacking solely military systems. The weapon might even possess an expanded target list, including civilian targets, following a valid collateral damage estimate. Cyberweapons deliberately created to seek out a specified set of targets comply with the laws of war, because decision-making process takes place during the cyberweapon's design phase, accomplished by a human and subject to an *ex ante* compliance analysis under LOAC.

Conversely, where computers exercise any level of autonomy in selecting additional targets, they slowly inch towards the other end of the spectrum. The software employs "inductive reasoning about characteristics of lawful targets not

---

[52] *See, e.g.*, Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, June 17, 1925, 26 U.S.T. 571, 94 L.N.T.S. 65; Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, Apr. 10, 1972, 26 U.S.T. 583, 1015 U.N.T.S. 163; Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, Jan. 13, 1993, 32 I.L.M. 800 (1993).

[53] Brown, *supra* note 32, at 195. By some states' definitions, so are nuclear weapons. The International Committee of the Red Cross purports that all uses of nuclear weapons would entail indiscriminate effects and thus be prohibited. During the 1995 *Nuclear Weapons* case before the International Court of Justice, Australia, Ecuador, Egypt, Iran, Japan, Lesotho, Malaysia, the Marshall Islands, Nauru, New Zealand, Rwanda, the Solomon Islands, Sri Lanka, Switzerland, and Zimbabwe adopted the position that LOAC prohibits the use of nuclear weapons. *See* Int'l Comm. of the Red Cross, *Practice Relating to Rule 71—Weapons That Are by Nature Indiscriminate*, *available at* http://www.icrc.org/customary-ihl/eng/docs/v2_rul_rule71 (last visited June 9, 2013); Legality of the Threat or Use of Nuclear Weapons (July 8, 1996), I.C.J. Reports 226, *available at* http://www.unhcr.org/refworld/docid/4b2913d62.html.

[54] The Law of Cyber-Attack, *supra* note 10, at 851.

already on the list," and compares these qualities on the fly.[55] Heuristics, in this scenario, examine additional targets using built-in parameters. This practice essentially amounts to the computer-based equivalent of procedurally identifying a target, which the laws of war allow. In fact, unlike determining whether a putative enemy possesses hostile intent, or whether aircraft intend to launch a strike, procedural identification in cyberspace might even be easier.

Standard objections against autonomy in weapons systems have traditionally focused upon the anecdotal scenario of robotic combatants attempting to distinguish between combatants and civilians, a scenario not so far-fetched, if one believes Russian press releases.[56] But when dealing only with computers, this question of deducing intent changes significantly: the decision-making takes place during software design, and the computer merely follows the programmer's code. After deployment, cyberweapons often can swiftly identify their targets' function and discern whether the computer is, for example, a Web server, an e-mail server, a Windows-based computer attached to network, or a SCADA-based controller for a hydroelectric dam. Moreover, they can also discern to which network a target belongs (e.g., civilian or military), and decipher how that network is mapped.[57]

The fewer built-in engagement parameters, the more unchecked automation the weapon possesses. And this kind of autonomy places the cyberweapon firmly towards the end of the spectrum (represented by computer viruses) prohibited by the laws of war due to its indiscriminate nature. Respecting the principle of distinction requires that cyberweapons boast a robust targeting algorithm fully vetted prior to employment. In these cases, special scrutiny must be directed towards the ability of the system to "learn" and adapt.

The role for lawyers and technologists is with heuristics. Heuristics are lawful, provided the weapon consistently employs preprogrammed parameters that restrict its targeting.[58] But this requires a thorough examination of how cyberweapons procedurally identify a potential lawful target. For instance, when computer scientists disassembled Stuxnet, they uncovered a mixed bag. The worm contained code that destroyed uranium-enriching centrifuges only physically located at Natanz, designed

---

[55] *Id.*

[56] Human Rights Watch, *supra* note 38, at 31-32.

[57] One scholar suggests that "marking" military computer systems with purely electronic identifiers, much as other protected sites are labeled under the Geneva Conventions, could aid in respecting the principle of distinction. Searching for electronic markers could be built into even an autonomous cyberweapon's heuristics, aiding their targeting. Brown, *supra* note 32, at 196.

[58] LOAC does not require the installation of "ethical governors" that prohibit weapons from attacking civilian systems, but it does require that protections against indiscriminate targeting, if created and applied to a weapon, not be subject to equally indiscriminate "rewriting." *See, e.g.*, Heather Roff, *When U.S. Weapons Are Autonomous, Who is Responsible?*, Huffington Post: Canada (Sept. 27, 2012), http://www.huffingtonpost.ca/heather-roff/the-dods-new-moral-code-f_b_1910608.html.

to reduce collateral damage if Stuxnet spread elsewhere, which it eventually did—all across the globe.[59] However, in order to distinguish between computers within the Natanz facility itself, the code detected whether the computer ran Siemens' Simatic Step7 software, which controls machines used for industrial production.[60] If the computer ran Step7, Stuxnet infected its target. Fortunately, though Stuxnet even spread to companies like Chevron, it withheld delivering its payload.[61]

Thus, Stuxnet's rudimentary targeting algorithms could have been improved, but at least they seemingly worked as intended. In short, assuming something akin to Stuxnet was a military-grade cyberweapon, LOAC permits its deployment when the principle of distinction is adequately respected. In carrying out its attack, the weapon may even gather identifying information about other systems it encounters. Further, the laws of war permit striking new, potential targets after comparing them to built-in parameters. But it cannot adjust those original parameters based upon new information, as this kind of decision-making shifts the cyberweapon away from the spectrum depicted above and towards a scenario where the machine itself effectively reviews its own proposed changes to targeting parameters. Doing so abrogates any review process entirely, and this situation must be avoided.

### C. Respecting the Principle of Proportionality

The *in bello* legality of a weapon also depends upon the principle of proportionality, codified in Articles 51(5)(b) and 57(2)(iii) of Additional Protocol I. This constraint upon a weapon's use prohibits attacks that "may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[62] An additional constraint, enumerated in Article 51(4)(a), prohibits operators from launching indiscriminate attacks, or those which tend to strike both lawful and prohibited targets without distinction.[63]

---

[59] Dan Goodin, *Puzzle Box: The Quest to Crack the World's Most Mysterious Malware Warhead*, Ars Technica (Mar. 14, 2013), http://arstechnica.com/security/2013/03/the-worlds-most-mysterious-potentially-destructive-malware-is-not-stuxnet/.

[60] *Id.*

[61] Michael Lee, *Stuxnet Infected Chevron, Achieved Its Objectives*, ZDNet (Nov. 9, 2012), http://www.zdnet.com/stuxnet-infected-chevron-achieved-its-objectives-7000007144/.

[62] AP1, *supra* note 22, art. 51(5)(b).

[63] This varies from, colloquially speaking, weapons that cannot be aimed, and instead prohibits an attacker himself from targeting the civilian population. A qualifying example would be dropping munitions upon a state's center of government, where the collateral damage would extend well into the civilian population. *Id.* art. 85(3)(a). Note that indiscriminate attacks are different from attacks that do not discriminate: the former deals with unnecessarily excessive collateral damage; the latter focuses on attacks that cannot tell the difference between lawful and prohibited targets, irrespective of the level of damage inflicted. *See* The Law of Cyber-Attack, *supra* note 10, at 850. n.130.

In other words, LOAC requires a balancing test prior to a weapon's employment, one which essentially disallows "overkill." This calculus limits the application of force, which may be used only "to the extent necessary for winning the war."[64] Assuming that a given cyberweapon can effectively distinguish between prohibited and lawful targets, their employment still invites uncertainty and doubt. For example, disrupting an American military unit's access to the Internet would be permissible under LOAC. However, the vast majority of unclassified Internet traffic conducted by the U.S. military to sustain its day-to-day operations runs along commercial lines. If an adversary's piece of malicious code inadvertently disrupts civilians' access to the Internet, does it constitute a violation of the laws of war? Using another example, what about hacking into command and control systems that operate conventional weapons and introducing errors that prevent weapons from test-firing?

With a twist of irony, the second example respects both fundamental principles of LOAC. It solely targets a military computer network and creates no immediately discernible spillover effect onto the civilian population, even though introducing software errors leading to potential misfires could prove catastrophic. Conversely, the Internet outage example demonstrates an immediate, unintended, and deleterious effect upon the civilian population, even absent much risk to the lives and property of civilians.

Computer networks route information; the impact of a weapon depends on what information they carry. As Professor Charles Dunlap noted, pragmatic concerns wholly independent of legal rules play an important role here, and decision-makers should assess the policy impacts of wholly permissible cyber-attacks.[65] Still, the interconnectedness of systems confounds the proportionality analysis.

While LOAC requires balancing military advantage against the adverse effect upon the civilian population, without sufficient information about the target and its connected systems, this calculus is almost impossible to achieve.[66] Situational awareness must be obtained prior to a weapon's employment. It must be updated continuously throughout its usage. And, crucially, there may be cases where operators cannot successfully assess the breadth of a targeted computer network or gauge the

---

[64] Human Rights Watch, *supra* note 38.

[65] Baker & Dunlap, *supra* note 31.

[66] Brown, *supra* note 32, at 60. Moreover, LOAC further prohibits targeting objects necessary for the survival of the civilian population, such as irrigation works, agricultural areas, and livestock. AP1I, *supra* note 22, art. 54. And, while a lengthy disruption of Internet services would not impact the survival of the human race, the United Nations has nevertheless affirmed Internet access as a basic human right. United Nations, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/HRC/17/27 (May 16, 2011), *available at* http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf. This suggests that greater weight should be given to civilians' continued access to Internet connectivity—at the very least, affording it the same protection as livestock.

anticipated effects of a successful attack. In such cases, LOAC prohibits launching the cyberweapon without more reliable intelligence.

Professor Michael Schmitt discusses the possibility of equipping autonomous weapons systems with sensors that identify targets and notes that human designers could bake this functionality into the weapon system.[67] As with the principle of distinction, heuristics may discern legitimate targets. The chief difficulty arises from how systems link together—in other words, "collateral computer damage." A secondary, equally troubling concern focuses on what the computer controls; this is important for those computers that run critical infrastructure sites, such as nuclear power plants, dams, sewage systems, air traffic control systems, and railways.

Programmatic constraints, in some respects, lessen this risk. For instance, software can sift between data, analyze its content, and permit the trafficking of unassociated civilian communications. Simultaneously, it could restrict the flow of combatants' data, in a sort of smaller version of China's Great Firewall. One scholar suggests that military systems be required to "mark" their traffic, systems, and networks electronically, much as traditional military forces are required to wear uniforms that distinguish them from civilians.[68] Such a framework would, if implemented, drastically reduce the risk of collateral computer damage, provided other belligerents played by the rules.

Similarly, cyberweapons could scout the targeted system and identify connected computers before launching a malicious payload. If the weapon encounters connected civilian computers, it could query its operator before assailing its target; if no such collateral damage concern exists, it would proceed accordingly. When a target pursued by operators using conventional weapons is not identified on a previously vetted list, problems multiply.[69]

Similar issues arise when cyberweapons see connected systems not previously accounted for, meaning that minimizing collateral computer damage requires the employment of programmatic safeguards. First, although a cyberweapon may initially be launched at a relatively isolated computer network, such as various secured networks employed by the American military, things have a tendency to spread—this is how Stuxnet infected Chevron after besieging Iran. Thus, weapons designers must account for this possibility. Launching the equivalent of an indiscriminate computer virus into a secured network might pass a *prima facie* test under

---

[67] Michael N. Schmitt, *Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics*, Harvard National Security Journal Feature (2013), *available at* http://ssrn.com/abstract=2184826.

[68] Brown, *supra* note 32, at 196.

[69] Jeffrey S. Thurnher, *No One at the Controls: Legal Implications of Fully Autonomous Targeting*, Joint Forces Quarterly no. 67, 77-84 (Oct. 2012), http://www.dtic.mil/dtic/tr/fulltext/u2/a564052.pdf.

LOAC, but the risk of collateral damage is too great. Second, these safeguards must exist prior to deployment. For instance, if the weapon interrupts communications, it should nevertheless allow messages from and to prohibited targets to continue. And when the weapon disrupts or degrades computers attached to a given network, it should assess the nature of all connected nodes: some innocent nodes may be classified as acceptable collateral damage, but this is not guaranteed. Even the mere presence of unidentified systems could impact whether to continue an attack. In short, if the weapon encounters a use case for which its designers had not planned, it must pause and await further human input.[70]

Smartly designed systems will require human input when the envisioned target possesses the ability to cause immediate, deleterious spillover into the civilian population (e.g., power plants, sewage systems, and hydroelectric dams). In other words, the greater the risk of immediate damage to the civilian population, as defined by traditional collateral damage assessments, the less cyberweapons should rely upon autonomous systems without human oversight. Under this analysis, malware like Stuxnet should possess thoroughly reviewed levels of decision-making capability, have discrete use cases which military planners can analyze prior to deployment, and boast ample safeguards that protect unintended targets from receiving the weapon's malicious payload.

### D. An Inevitable Use Case: Attacking Dual-Use Structures at the Outset of Hostilities

Even if certain cyberweapons pass those initial hurdles, just like the bomber pilot dropping ordnance, they must be aimed appropriately and take possible collateral damage into consideration. Cyber-attacks have "advanced to the point where military forces now have the capability to inflict injury, death, and destruction via cyberspace" without putting human combatants in harm's way.[71] The weapons are novel; so are the laws circumscribing their usage. More to the point, at the beginning of hostilities, it is axiomatic that cyberweapons have a crucial role to play, as they did in Estonia in 2007. In April of that year, unknown elements inside Russia employed a botnet that struck nearly the entire country's electronic infrastructure, leaving Estonian information technology specialists with one option: cutting off the world to the country's domestic networks.[72] Approximately two weeks later, the botnets stopped, shifting gears to other tactics, such as sending spam worldwide.[73]

---

[70] Note that this criterion requires operators not anticipating the scenario at all: if the weapon encounters an envisioned scenario, even one defined by "if-then" statements baked into the software, it may continue without interruption.

[71] Brown, *supra* note 32, at 180.

[72] Häly Laasme, *Estonia: Cyber Window into the Future of NATO*, Joint Forces Quarterly no. 63, 58-63 (Oct. 2011), *available at* http://www.hsdl.org/?view&did=689675.

[73] Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED (Aug. 21, 2007), http://archive.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

Although Moscow officially eschewed involvement with the coordinated attack, it hardly stretches the imagination to imagine the strike as a self-terminating warning shot launched across the bow of Estonia's digital domain. More importantly, even taking Russia's words at face value and assuming that Russian hackers merely coordinated their efforts, it was a successful proof of concept: Tallinn's banking sites and internal government servers were overloaded and rendered useless.[74] And that merely invites one to ponder the efficacy of a similar, state-sponsored attack.

Already, DoD specifically envisions attacks upon America's critical infrastructure—and surely plans on attacking adversaries' infrastructure as well. Weapons like Plan X contemplate disruptions to Internet service, which nearly everyone uses, including military entities. This is only natural, as cyberwarfare generally spares soldiers' lives and requires no expenditure of materiel or ordnance, only bandwidth. Moreover, as seen with Stuxnet and in Estonia, cyberweapons can achieve military objectives without causing damage comparable to traditional kinetic attacks.[75] Theoretical examples of possible objects of cyberwarfare include targeting:

> [A]n electric utility . . . to affect a power grid that supplies a telecommunications company used to attack the attacker. Or a transportation system could be subjected to repeated, apparently random attacks to create a loss of confidence in the government. Similarly, hospital or school databases could be attacked to disrupt activities at the heart of . . . personal security.[76]

The Government Accountability Office (GAO), the agency responsible for providing nonpartisan investigative reports to Congress in a watchdog capacity, has for years now consistently warned lawmakers against the brittleness and vulnerability of America's critical infrastructure.[77] Other nations' infrastructure—potential targets—likely suffer from similar debilitations.

---

[74] *Id.*

[75] Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts*, 43 Vand. J. Transnat'l L. 1011, 1013 (2010) (citing Arie J. Schaap, *Cyberwarfare Operations: Development and Use Under International Law*, 64 A.F. L. Rev. 121, 158 (2009) ("[B]enefits include less physical destruction, less cost than other types of traditional warfare, and the ability to still achieve the same results with less risk to military personnel.")); Jeffrey T.G. Kelsey, Note, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, 106 Mich. L. Rev. 1427, 1440-41 (2008) ("Unlike a conventional attack, a cyber attack could neutralize . . . targets without causing physical injury to the civilians or physical damage to the site."); Dorothy E. Denning, *Barriers to Entry: Are They Lower for Cyber Warfare?*, IO Journal, Apr. 2009, at 6-10 (explaining that the effects of cyber weapons are less devastating than those of kinetic warfare because cyberwarfare more indirectly results in death and often produces more short-term effects).

[76] Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Casualties*, 13 SMU Sci. & Tech. L. Rev. 249, 252 (2010).

[77] U.S. Government Accountability Office, *supra* note 27.

But attacks upon critical infrastructure can cause ample damage, sometimes unintentionally. Consider a malfunction in Stuxnet that, instead of shutting down Iranian reactors, instead caused them to explode. In those cases, cyber-attacks could constitute violations of the laws of war.[78] Moreover, the proliferation of dual-use facilities and systems complicates the ability of cyberweapons to limit their effects solely to lawful targets.[79] Of course, not all targets are lawful ones: LOAC prohibits combatants from directly attacking places like hospitals and schools. For instance, where the "destruction of bridges, railroads, communications centers, and fuel supplies . . . offers a definite military advantage," those facilities have historically been considered lawful targets if deemed part of military infrastructure.[80]

But telecommunications systems prove more troubling, and yet they will inevitably appear on target lists anyway. Doing so undoubtedly achieves the conditions of "cyberspace superiority," which DoD doctrine recognizes as crucial for enabling freedom of action and maximizing commanders' options.[81] Few could argue that shutting down access to the Internet and banking sites for two weeks is bloodier and more "warlike" than dropping bombs.

Although DoD information flows across secure, military-restricted networks, which would undoubtedly qualify as lawful targets, much of its general, day-to-day network traffic routes through the unclassified Internet. The same goes for information from senior civilian officials. The recent imbroglio concerning General David Petraeus, the former director of the Central Intelligence Agency, demonstrated that clandestine messages sometimes pass through publicly available systems.[82] Does this make commercial e-mail servers, such as Google, valid military

---

[78] Brown, *supra* note 32, at 188 ("An act that violates LOAC if carried out by conventional means also violates LOAC if carried out by an information attack. Obversely, an act that is not a war crime if carried out by conventional means cannot be converted to one if accomplished electronically.").

[79] The Law of Cyber-Attack, *supra* note 10, at 852-53. This area of the law remains unsettled and ripe for disagreements.

> The circumstances under which an attack on a dual use target is legal under the LOAC are nebulous, to say the least. . . . [A]n attack may still run afoul of Protocol I's provisions if it is indiscriminate; it might not be limited to solely military objectives or the impact might be disproportionately felt by the civilian population. There is a divergence of opinion among commentators, particularly regarding proportionality--some maintain that only direct civilian casualties resulting from an attack should be considered, while others would include all indirect effects and collateral damage, which can be substantial even in targeted attacks like Stuxnet.

Scott J. Shackelford & Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 Geo. J. Int'l L. 971, 1004-05 (2011).

[80] Brown, *supra* note 32, at 193-94.

[81] JP 3-0, *supra* note 30, at V-48.

[82] Max Fisher, *Why David Petraeus's Gmail Account is a National Security Issue*, Wash. Post (Nov. 10, 2012), http://www.washingtonpost.com/blogs/worldviews/wp/2012/11/10/why-david-petraeuss-

targets? What about Tier 1 Internet Service Providers that route unclassified military network traffic as well as the average citizen's?

Presumably the answer depends on whether an attack against its servers aims to disrupt, degrade, or destroy them. The lawfulness of attacks on dual-use facilities turns on "whether the military advantage gained by attacking the target outweighs the adverse effect on civilians and the civilian population."[83] In conventional warfare, states might merely restrict the general population from depots or military bases, as LOAC requires sequestering civilians and their property from possible military objectives.[84] However, when that separation is unfeasible, dual-use structures are subject to attack.

With computer networks, this invites broad levels of permissibility. One scholar even suggests that because "95% of all U.S. military traffic moved over civilian telecommunication and computer systems," all computer networks are fair game.[85] This realization places the question squarely within the domain of proportionality, which itself turns upon the calculus between the anticipated military advantage and the expected loss to civilian objects. This Article submits that, much like how the synthesis of greater autonomy and fewer engagement parameters makes a cyberweapon more virus-like (and thus prohibited), an attack that fails to adjust in response to changes in military advantage fails to respect the principle of proportionality.

For better or worse, the attacks levied against Estonia were the "right" way to fight: they targeted government computers, crippled the country's economic mobilization by denying access to banking sites and ATMs, and they managed to avoid hampering impermissible critical infrastructure site like hospitals. More importantly, unlike the titular Terminators of the movie franchise, the attacks self-terminated as the perceived military advantage lessened—that is, after the aggressors proved their point. This fact hammers home the impermissibility of virus-like autonomous cyberweapons for another reason: they possess the risk to cross into dual-use structures but lack the ability to adjust to military necessity.[86]

---

gmail-account-is-a-national-security-issue/.

[83] Brown, *supra* note 32, at 194.

[84] AP1, *supra* note 22, art. 58.

[85] Hollis, *supra* note 33, at 1044.

[86] Attacks "which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated," are prohibited and deemed indiscriminate. AP1, *supra* note 22, art. 51(5)(b).

E. The Necessary Safeguards to Ensure Autonomous Cyberweapons' Legality

Cyberweapons are, by definition, perfectly controllable. They follow the instructions of their code without fail; any randomness injected into their programming is by conscious design or programmer oversight. In this sense, autonomy in cyberweapons seems something of a misnomer: if computers "learn," they do so by exercising learning algorithms. And these algorithms can be designed to respect the laws of war.[87] As noted above, LOAC would only outright prohibit cyberweapons without any programmatic constraints, with the remaining types of weapons evaluated on a case-by-case basis.[88] Conducting an individualized evaluation of cyberweapons must involve a thorough analysis of its programming, and this analysis must verify that a given cyberweapon possesses those necessary safeguards.

First, in order to respect the principle of distinction, the weapon must adequately differentiate between permissible and prohibited targets. It could employ a previously vetted list of targets or rely instead upon heuristics that dynamically assess whether a potential target conforms to prescreened parameters, such as running a certain piece of software or being physically located in a given area. This second case requires heightened legal scrutiny, but could nevertheless comply with the laws of war. However, cyberweapons cannot adjust these preprogrammed heuristics, or engagement parameters, through adaptive learning alone. They must instead reach back to the operators for human input.[89]

Second, concerning the principle of proportionality, cyberweapons must, to the maximum extent possible, limit both "collateral computer damage" and real, physical damage caused by computer failure. In the first case, data can be sifted and analyzed, allowing civilians' information to continue flowing while combatants' data screeches to a halt. Such a framework accounts for attacks upon telecommunications networks. In the second case, concerning other critical infrastructure sites—such as electrical facilities or water distribution systems—a collateral damage assessment must be conducted prior to a weapon's employment.

In sum, faulty heuristics might lead to unintended engagements. Or they could lessen risks by providing operators with additional situational awareness, just like targeting pods on fighter aircraft or night vision goggles.[90] The risk of Stuxnet's

[87] Brown, *supra* note 32, at 196.

[88] *See* Schmitt, *supra* note 67, at 7.

[89] Deciding whether a target conforms to certain level of prescreened qualities, thus marking it as a target, essentially means pausing and examining the data on the targeted system, or examining the data trafficked between that system and others. If, in doing so, the cyberweapon encounters an e-mail server associated with the military or government, it could check its built-in parameters and realize that target is lawful. Conversely, dynamic updating of parameters goes beyond simple "if-then" comparisons. Rather, it involves the cyberweapon itself adding levels of comparison through assessing the battlespace—otherwise stated, by "learning."

[90] DoD intends for computer systems autonomously to perform tasks like "generating optimal

successful deployment is that it could set bad precedent. Fully autonomous, "fire and forget" software requires the most stringent oversight. In the ideal case, well-designed autonomy can actually increase compliance with the laws of war.[91] But the weapons must be specifically designed to take advantage of those technological advances, and they must be fully vetted prior to deployment.

## II. THE ROLE OF CIVILIANS AND CONTRACTORS IN THE DESIGN OF AUTONOMOUS CYBERWEAPONS

In recent years the sharp divide between the roles performed by civilians and by military members has lessened. Civilians regularly serve as directors of military entities, and they often maintain an outsized role in government procurement actions. The twenty-first century brought with it a "growing military dependency on civilians, and on civilian objects and activities."[92] That dependence includes utilizing civilians to perform historically "military" roles, such as providing security during peacekeeping efforts. In certain cases, this shift has not gone unchallenged. For example, the use of private security contractors in regions characterized by hotbeds of conflict, such as in Iraq and Afghanistan, drew ample scrutiny.[93]

Conflict zones in cyberspace have thus far escaped similar attention, chiefly due to their novelty and the lack of broad consensus on how the laws of war apply to civilians participating in cyber-attacks. However, the duties performed by civilians and contractors will undoubtedly acquire increasing importance. Uniformed military forces cannot meet the challenges of the twenty-first century alone. Their numbers simply do not allow for that luxury.

In the near future and perhaps beyond, private contractors and civilians will furnish support and possibly conduct cyber operations.[94] Only combatants may employ weapons and wage war. But cyberweapons may be divided into three distinct elements—the code, the computer system, and the operator's input—and

---

plans, monitoring plan execution and problem solving, selecting or allocating resources, analyzing data or imagery, implementing or activating the next step in the plan, reacting to the environment to perform the best action and learning." U.S. Dep't. of Def., Task Force Report: The Role of Autonomy in DoD Systems 21 (July 2012) [hereinafter Autonomy Report], *available at* http://www.acq.osd.mil/dsb/reports/AutonomyReport.pdf. Note, however, that DoDD 3009.09 was released months later, in November 2012. *See supra* note 2.

[91] Waxman, *supra* note 32, at 444.

[92] Michael N. Schmitt, *Bellum Americanum: The U.S. View of Twenty-First Century War and Its Possible Implications for the Law of Armed Conflict*, 19 Mich. J. Int'l L. 1051, 1068 (1998).

[93] *See, e.g.*, Christopher M. Kovach, *Cowboys in the Middle East: Private Security Companies and the Imperfect Reach of the United States Criminal Justice System*, Connections, vol. IX, no. 2 (2010), *available at* http://connections-qj.org/system/files/09.2.02_kovach.pdf?download=1.

[94] Nils Melzer, *Cyberwarfare and International Law: Ideas for Peace and Security* 34 (2011), *available at* http://unidir.org/pdf/activites/pdf2-act649.pdf.

all are subject to the laws of war.[95] Thus, the integration of civilians into military operations waged by cyberweapons raises a salient question: do the laws of war restrict what designers of civilian cyberweapons may do?[96]

A. An Overview of Civilians' Protected Status under LOAC

The principle of distinction, which protects civilians from being the object of attack, forms the bedrock principle of the laws of war, illustrated by the Additional Protocol to the Fourth Geneva Convention of 1949. The Convention also dictates that only combatants may lawfully take part in hostilities.[97] Since LOAC recognizes no geographical limitations, this restriction applies equally in cyberspace.

Article 50(1) of the Additional Protocol illustrates that a civilian is "any person who does not belong to one of the categories of persons referred to in Article 4 (A) (1), (2), (3), and (6) of the Third Convention and in Article 43 of this Protocol."[98] Moreover, unless one falls within these exclusions, they are considered civilians by default. As Professor Schmitt explains, this distinction between combatant and civilian is binary, for they are "opposite sides of the same coin."[99] Article 43(1) of the Additional Protocol provides that:

> [T]he armed forces of a Party to a conflict consist of all organized armed forces, groups and units which are under a command responsible to that Party for the conduct of its subordinates, even if that Party is represented by a government or an authority not recognized by an adverse Party. Such armed forces shall be subject to an internal disciplinary system which, *inter alia*, shall enforce compliance with the rules of international law applicable in armed conflict.[100]

Moreover, Article 43(2) of the Additional Protocol explicitly defines combatants as "[m]embers of the armed forces of a Party to a conflict (other than medical personnel and chaplains)"[101] Upon first glance, this definition suggests that only uniformed members of the armed forces qualify as lawful combatants, and that only combatants may launch cyber-attacks. But, other sources extend the definition.[102] The relevant

---

[95] Brown, *supra* note 32, at 184.

[96] For a thorough analysis of the evolution of international law concerning the protection of civilians during times of war, *see* Brenner & Clarke, *supra* note 75, at 1015-24.

[97] AP1, *supra* note 22, art. 51.

[98] *Id.* art. 50(1).

[99] Michael N. Schmitt, *Humanitarian Law and Direct Participation in Hostilities by Private Contractors or Civilian Employees*, 5 CHI. J. INT'L L. 511, 523 (2005).

[100] AP1, *supra* note 22, art. 43.

[101] *Id.*

[102] Brenner & Clarke, *supra* note 75, at 1022.

parts of Article 4 of the Third Geneva Convention of 1949 exempt the following from civilian status:

> (1) Members of the armed forces of a Party to the conflict as well as members of militias or volunteer corps forming part of such armed forces.
>
> (2) Members of other militias and members of other volunteer corps, including those of organized resistance movements, belonging to a Party to the conflict and operating in or outside their own territory, even if this territory is occupied, provided that such militias or volunteer corps, including such organized resistance movements, fulfill the following conditions:
>
> (3) that of being commanded by a person responsible for his subordinates;
>
> (a) that of having a fixed distinctive sign recognizable at a distance;
> (b) that of carrying arms openly;
> (c) that of conducting their operations in accordance with the laws and customs of war.[103]

Satisfying the above criteria grants prisoner-of-war (POW) status.

Article 4(A)(1) addresses combatant status that occurs after formal incorporation by the state, or *de jure* status, whereas Article 4(A)(2) confers combatant status merely based upon the group's collective actions.[104] And, because these four criteria also apply to groups created under Article 4(A)(1), as they constitute an implicit definition of the armed forces, they further restrict those who might wage war after formal incorporation by the state.[105] Article 43(3) adds another critical restriction to this process, proscribing that "[w]henever a Party to a conflict incorporates a paramilitary or armed law enforcement agency into its armed forces it shall so notify the other Parties to the conflict."[106] Absent proper incorporation and notification, paramilitary organizations act outside the law.[107]

---

[103] Geneva Convention (III) Relative to the Treatment of Prisoners of War art. 4, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter GC3]. The Additional Protocol to Geneva Convention (IV) also details those persons eligible for prisoner-of-war status. AP1, *supra* note 22, arts. 43-44. The same conditions also appear in the Fourth Hague Convention. *See* Hague Convention (IV) with Respect to the Laws and Customs of War on Land annex, art. 1, Oct. 18, 1907, 36 Stat. 2277, 187 Consol. T.S. 429.

[104] Schmitt, *supra* note 99, at 523-24.

[105] *Id.* at 525.

[106] AP1, *supra* note 22, art. 43(3).

[107] Schmitt, *supra* note 99, at 525 ("This makes it patent that unincorporated paramilitary and law

Thus, barring formal recognition and incorporation by the state (which is proved by such factors as enlistment contracts, oaths of office, and wearing distinctive uniforms), civilians cannot readily enjoy Article 4(A)(1) protection. Indeed, "some countries require certain civilian employees in key positions to serve as [military] reservists; this facilitates their rapid change of status in the event of armed conflict."[108] Civilians not occupying such positions could readily be viewed as lacking Article 4(A)(1) status.

On the other hand, other paramilitary corps may carry out attacks and enjoy Article 4(A)(2) protection, provided they "possess military command, control, and disciplinary characteristics analogous to the regular forces they join."[109] But this caveat, along with the four criteria described above, are not easily satisfied. Nor can the mere function such a group performs grant it the veneer of combatant status. In fact, one scholar suggests that because paramilitary and law enforcement groups must formally be incorporated to achieve combatant status, other groups of government employees must do the same, leaving them unable to merely rely upon the lesser requirements of Article 4(A)(2).[110]

Where does this leave those employees relevant for the purposes of this Article, such as non-uniformed civilians attached to the Department of Defense or computer network exploitation experts working for the Central Intelligence Agency? Unless formally attached and incorporated into the armed forces—with uniforms, a commander, and wielding rootkits openly—they cannot lawfully launch cyber-attacks.

It might be argued that, in many cases, these civilians merely accompany the armed forces and perform support functions. This category includes persons such as war correspondents, laundry crews, or supply contractors, and these persons receive POW status if captured.[111] However, they too possess no legal right to engage in

---

enforcement agencies are civilian in nature for the purposes of humanitarian law.").

[108] *Id.* at 524.

[109] Geoffrey S. Corn, *Unarmed but How Dangerous? Civilian Augmentees, the Law of Armed Conflict, and the Search for a More Effective Test for Permissible Civilian Battlefield Functions*, 2 J. Nat'l Sec. L. & Pol'y 257, 264 (2008).

[110] Schmitt, *supra* note 99, at 525. Note, however, that according to Schmitt, while this logic excludes groups of civilian employees from banding together to wage war—because of the incorporation requirement—the Article 4(A)(2) inquiry might apply to private contractors.

[111] GC3, *supra* note 103, art. 4(A)(4) ("Persons who accompany the armed forces without actually being members thereof, such as civilian members of military aircraft crews, war correspondents, supply contractors, members of labour units or of services responsible for the welfare of the armed forces, provided that they have received authorization, from the armed forces which they accompany, who shall provide them for that purpose with an identity card similar to the annexed model."). Other non-combatant civilians, such as those "taking no active part in the hostilities including members of the armed forces who have laid down their arms and those placed hors de combat by sickness, wounds, detention, or any other cause," qualify as "protected persons" and must receive other safeguards against inhumane treatment. Geneva Convention (IV) Relative to the

hostilities themselves.[112] While they may become casualties due to their proximity to the armed forces, they are not lawful *targets* due to their relationship to the armed forces.[113] The commentary to the Additional Protocol formalizes this divide:

> All members of the armed forces are combatants, and only members of the armed forces are combatants. This should therefore dispense with the concept of "quasi-combatants," which has sometimes been used on the basis of activities related more or less directly with the war effort. Similarly, any concept of a part-time status, a semicivilian, semi-military status, a soldier by night and peaceful citizen by day, also disappears. A civilian who is incorporated in an armed organization . . . becomes a member of the military and a combatant throughout the duration of the hostilities . . . .[114]

In sum, only members of the armed forces or other corps associated with the military that respect traditional command structures and fall within the regular forces' chain of command qualify as combatants.[115] Unaffiliated civilians and those offering benign support stand outside this paradigm; they are shielded from attack as long as they remain on the sidelines. However, when civilians—including those performing support functions—directly participate in hostilities, they lose this protection and may be targeted by hostile forces.[116] In such cases, they would be subject to criminal prosecution and could even be tried by military commission.[117]

Practically speaking, civilians may be involved in the design, maintenance, and some aspects of the operation of cyberweapons. Conventional computer-based attack and exploitation, such as hacking into an adversary's computer network to retrieve information, can constitute an attack under the laws of war. But autonomy complicates the question. For the first time in human history, decision-making algorithms that possibly implicate LOAC are designed in laboratories far removed from the battlefield, most often by civilian computer scientists.

---

Protection of Civilian Persons in Time of War art. 3(1), Aug. 12, 1949, 6 U.S.T 3516, 75 U.N.T.S. 287 [hereinafter GC4].

[112] Brown, *supra* note 32, at 191.

[113] Corn, *supra* note 109, at 267.

[114] Int'l Comm. of the Red Cross, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (Yves Sandoz et al. eds., 1987), at 515, *available at* http://www.icrc.org/ihl.nsf/WebList?ReadForm&id=470&t=com.

[115] Corn, *supra* note 109, at 267.

[116] AP1, *supra* note 22, art. 51(3); GC3, *supra* note 101, art. 4(A).

[117] Brenner & Clarke, *supra* note 75, at 1022-23.

B. The Unclear Status of Cyberweapons' Designers and Programmers

The combatant status of the operator of a cyberweapons (that is, the person seated at a computer console who, under the example of Plan X described above, chooses targets and deploys certain toolkits; or the person who launches the Stuxnet worm into the Natanz network), may be dispensed with fairly easily. Actively launching and directing the weapon unmistakably constitutes participation in hostilities and must be carried out by a lawful combatant. Equally simple are cases involving designers of conventional weapons systems. Traditionally, civilian weapons designers have not been deemed to have directly participated in hostilities, which would forfeit their protected status under LOAC.[118] The status of a vendor like Boeing selling fighter aircraft to the Air Force is clear: the designers qualify as unaffiliated civilians.

But designers of autonomous cyberweapons occupy murkier territory. To date, the United States has not promulgated unclassified documentation regarding the permissibility of possible non-combatants, such as designers developing software that will eventually be used in cyber-attacks.[119] Nor has international law kept pace with this edge case. In other words, the operative question is whether the designer of a cyberweapon invites exposure to LOAC merely by coding a weapon that possesses robust decision-making algorithms, which are later deployed by a third party. This question turns on whether such actions are deemed to constitute direct participation in hostilities, which makes these civilians both targetable by adverse parties and punishable for their crimes. And unfortunately, that term is not defined by treaty law.[120]

The United States, for its part, has traditionally defined "direct participation in hostilities" rather broadly. In 2002, although it has not ratified the base Convention on the Rights of the Child, the United States acceded to the Optional Protocol on Involvement in Armed Conflict.[121] In doing so, the United States issued an understanding regarding the treatment of the term.[122] Under this view, which stresses the

---

[118] The Law of Cyber-Attack, *supra* note 10, at 853.

[119] It has, however, restricted the participation of the National Guard. National Guardsmen must be in "federal" status before participating in cyber-attack missions. *See supra* note 23. Of course, Guardsmen—even if in "state" status—would still be considered combatants. In other words, this prohibition is more an attempt to conform to ensure cleaner lines of command, as in certain cases National Guardsmen are bound to follow the orders of the governor of their home state.

[120] Nils Melzer, Int'l Comm. of the Red Cross, Interpretive Guidance on The Notion of Direct Participation Under International Humanitarian Law 41 (2009), *available at* http://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf.

[121] Optional Protocol to the Convention on the Rights of the Child on the Involvement of Children in Armed Conflict art. 1, May 25, 2000, 2173 U.N.T.S. 222.

[122] The understanding states that, with respect to Article 1 of the Protocol,

causal relationship between one's actions and the effect upon the battlefield, the efforts of civilian weapons designers might qualify as direct participation:

> Suppose, however, that instead of building off-the-shelf CNA [computer network attack] tools, the programmer designs destructive code, custom-built to the intelligence mapped by the computer reconnaissance expert. Imagine further, that he works closely with the mapper and routinely adjusts or tweaks the code, up to the moment of attack. Such efforts ensure that the CNA leverages the most recent intelligence and produces exactly the attacker's intent, including a minimization of collateral damage and casualties . . . . *The CNA weapon designer also may strain the boundaries of permissible civilian contributions to combat*.[123]

The International Committee of the Red Cross (ICRC) has offered further nonbinding guidance on this question of unsettled law. According to its criteria, a specific act must meet the following criteria to qualify as direct participation in hostilities:

> (1) the act must be likely to adversely affect the military operations or military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack (threshold of harm), and
>
> (2) there must be a direct causal link between the act and the harm likely to result either from that act, or from a coordinated military operation of which that act constitutes an integral part (direct causation), and
>
> (3) the act must be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another (belligerent nexus).[124]

---

> [t]he United States understands the phrase 'direct part in hostilities' to mean immediate and actual action on the battlefield likely to cause harm to the enemy because there is a direct causal relationship between the activity engaged in and the harm done to the enemy. The phrase 'direct participation in hostilities' does not mean indirect participation in hostilities, such as gathering and transmitting military information, transporting weapons, munitions, or other supplies, or forward deployment.

Message from the President of the United States Transmitting Two Optional Protocols to the Convention on the Rights of the Child, S. Treaty Doc. No. 106-37, at VII (2000).

[123] Sean Watts, *Combatant Status and Computer Network Attack*, 50 VA. J. Int'l. L. 391, 429 (2010) (emphasis added).

[124] Melzer, *supra* note 120, at 16.

Following these criteria, in the ICRC's view, both computer network attack and computer network exploitation would count as direct participation.[125]

The Program on Humanitarian Policy and Conflict Research (HPCR) at Harvard University released additional commentary on this subject, noting that when computer-based operations "directly cause death, injury or destruction, or system malfunctions adversely affecting the military capacity or military operations of the enemy," they qualify as direct participation.[126]

Conversely, "indirect" participation in hostilities—or being part of the general war effort—does not deprive civilians of their protected status. This would not only include innocuous actions like buying war bonds or participating in rationing programs, but also conducting scientific research and design.[127] The ICRC stresses the importance of directness, noting that even assembling and storing a weapon such as an improvised explosive device (IED) would not count as direct participation, even though an uninterrupted causal link exists between the weapon's creation and its detonation.[128]

Regrettably, the case of programmers of autonomous cyberweapons (or indeed, autonomous weapons generally speaking) remains unsettled. In this Article's view, the decision-making algorithms embedded within autonomous cyberweapons mandate different treatment for their designers. At this point, without consensus in the international community to give rise to customary international law or, more usefully, formal treaties, the most one can do is employ analogies. By looking at two well-known autonomous cyberweapons, one can assess whether, assuming their designers were civilians supporting a government's war effort, their efforts amounted to direct participation in hostilities.

First, recall that Stuxnet, in its simplest form, assessed its target's geographical location and determined whether the target ran industrial control software. If both questions were answered affirmatively, it launched its payload. Although

---

[125] *Id.* at 48-49.

[126] The Program on Humanitarian Policy and Conflict Research, Harvard University, Manual on International Law Applicable to Air and Missile Warfare (May 15, 2009), *available at* http://ihlresearch.org/amw/HPCR%20Manual.pdf. Curiously, however, the commentary to the Manual notes that merely hacking into a military base's intranet does not automatically qualify as participation in hostilities. The Program on Humanitarian Policy and Conflict Research, Harvard University, Commentary on the Manual on International Law Applicable to Air and Missile Warfare—Section F: Direct Participation in Hostilities, *available at* http://www.ihlresearch.org/amw/manual/category/section-f-direct-participation-in-hostilities [hereinafter HPCR Commentary].

[127] Melzer, *supra* note 120, at 53-54. But even this has limits, and the ICRC noted that in extreme situations, such as "where the expertise of a particular civilian was of very exceptional and particularly decisive value for the outcome of an armed conflict, such as the case of nuclear weapons experts during the Second World War." *Id.* at 53 n.122.

[128] *Id.* at 53-54.

strategic guidance was undoubtedly passed to the programmer, such as limiting the destructive payload to Iranian nuclear sites, the designer implanted that guidance at a tactical level. Not only did the programmer design the ruleset that identified the selected target, but that coder also chose that type of "warhead" that achieved the desired military effect.

Second, in the case of Gauss, a successor to Stuxnet, its programmers not only incorporated decision-making logic, such that only specifically targeted computers risk attack, but the weapon effectively employs stealth capabilities. On most computers, "the module remains cloaked in an impenetrable envelope that prevents researchers and would-be copycats from reverse engineering the code."[129] Because of this concealment, both the weapon's targeting mechanism and how it spreads from one computer to another remain hidden.

In both cases, programmers likely received strategic guidance from state actors, especially given the sophistication of the weapons. In Stuxnet's case, the strategy probably amounted to crippling Iran's nuclear program while ensuring other targets, if struck by the weapon, suffered no ill effects. After receiving this strategy, the programmers effectively conducted tactical-level planning, either alone or jointly with state sponsors. In the end, the weapon was programmatically bound by rules and criteria crafted by the coders.[130]

As the HPCR notes, "[i]ssuing orders and directives to forces engaged in hostilities; making decisions on operational/tactical deployments; and participating in targeting decision-making" are all forms of direct participation in hostilities.[131] This sort of tactical-level planning goes beyond the "decisions" that embedded systems in other weapons might take, such as the detonator attached to land mines; navigational aids that control the post-launch flight of missiles; or the radio receiver used in some forms of IEDs. Indeed, as Professor Schmitt suggests, civilians who "engage in tactical level planning or approval are directly participating in hostilities and thereby legitimate targets."[132]

The difference lies in the interface between the designer's will—via lines of code—to the capacity of the weapon itself to acquire and prosecute possible targets. In fact, target acquisition, which amounts to identifying possible sets of targets for engagement, is another commonly accepted example of directly participating in hostilities.[133] Moreover, with Gauss, elements of active concealment serve as further

---

[129] Goodin, *supra* note 59.

[130] Even easier is the case of programmers who modify code in preparation for an attack, because their efforts could constitute performing a continuous combat support function.

[131] HPCR Commentary, *supra* note 126.

[132] Schmitt, *supra* note 99, at 5443 (citing Michael N. Schmitt, *State Sponsored Assassination in International and Domestic Law*, 17 Yale J. Int'l L. 609 (1992)).

[133] HPCR Commentary, *supra* note 127.

evidence of specific, tactical action undoubtedly designed by the programmer to achieve some specific, operational goal.

Some might argue that the planning taking place in the Research and Development (R&D) lab constitutes only a preparatory measure, one far removed from the battlefield (especially in cases where a government commissions the creation of a weapon from a contractor). But even preparatory acts can qualify as participation in hostilities.[134] The question is naturally one of degree, and the examples in the ICRC's 2008 study distinguish between those measures and other functions which merely build the capacity to wage war. Notably, the ICRC's analysis relies upon a causal chain more than anything else; it cites loading bombs onto an airplane for an attack at an unspecified time in the future as direct participation, but exempts transporting bombs to a warehouse for future use by belligerents.[135]

In the case of autonomous cyberweapons, although the geographical and temporal link between a weapon's design and its deployment could be quite tenuous, neither of these factors diminishes the causal link between the programmer's tactical planning, the decision-making algorithms embedded in the code itself, and the effects the weapon inflicts. Indeed, if merely "transmitting tactical targeting information for an attack" qualifies as direct participation in hostilities, surely crafting exactly how a weapon operates does too.[136]

Unfortunately, the United States currently refrains from defining the concept of "autonomy" altogether. Instead, its Defense Department adopted a definition which solemnizes the symbiotic human-computer relationship, which rejects even the possibility of a fully autonomous system:

> The milestones and roadmaps based on computer functions needed for some level of autonomy—rather than to achieve a capability through the best combination of human and machine abilities—foster brittle designs resulting in additional manpower, vulnerabilities and lack of adaptability for new missions. Casting the goal as creating sophisticated functions—rather than creating a joint human-machine cognitive system—reinforces fears of unbounded autonomy and does not prepare commanders to factor into their understanding of unmanned vehicle use that there exist no fully autonomous systems, just as there are no fully autonomous soldiers, sailors, airmen or Marines.[137]

---

[134] Melzer, *supra* note 120, at 66.

[135] *Id.*

[136] *Id.* at 48.

[137] DoD Autonomy Report, *supra* note 90, at 23.

According to this approach, even the most automated systems are "joint human-machine cognitive systems."[138] When applied to enhanced navigation or targeting pods attached to aircraft; intelligence-gathering tools that parse copious amounts of raw data; or even something simpler, like spam filters on electronic mail servers, this rings true.

But as the example of Stuxnet illustrates, cyberweapons exercise internal judgment after being launched. In other words, the human element in cyberweapons may become increasingly further removed from the final impact. In these cases, a portion of the decision-making process is hard-coded into the system itself, such that operators and end users may not completely understand or even have the ability to fully control its inner workings. And hazily defined frameworks often invite criticism.[139]

C. The Responses from American Military Departments to this Dilemma

For the above reasons, this Article suggests that designers of autonomous cyberweapons could face LOAC exposure. Given this area's novelty, there exists no consensus regarding this question. But organizations within the United States government have nevertheless considered what limitations should be imposed upon civilians and contractors involved in the design and operation of cyberweapons. A 2010 memorandum from The Judge Advocate General of the Air Force to DoD's General Counsel "raised concerns about the insufficiency of DoD's policies to determine precisely what DoD civilian activities or duties were permissible in relation to computer network attack operations and, in the absence of clarification on these matters, recommended that Air Force leadership limit DoD civilian roles in such cyberspace operations." [140] And in conducting further investigations, the GAO noted in a 2011 report to Congress that Air Force officials responsible for its cyberspace program echoed this uncertainty, wondering whether Air Force civilians could even conduct cyber operations.[141] The Navy, on the other hand, took a more conservative approach and stated that its civilians only perform "support roles," but could expand their mission set depending upon future needs.[142] The GAO called for "a greater level of detail . . . with regard to the categories of personnel—military,

[138] *Id.* at 24.

[139] For instance, one commentator notes that DoD's "position presents a nice little loophole with which to stop debate about increased autonomy in weapons systems. The critic says, 'we worry about attributing responsibility to a weapon that decides to fire on a target by itself.' The DoD responds 'there is a human-machine cognitive system, and so don't worry, there is a human there!' But the question remains: where? How far removed is this person? The commander? The General? The President?" Roff, *supra* note 58.

[140] U.S. Government Accountability Office, Department of Defense Cyberspace Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities, GAO-11-421, 13 (May 2011), *available at* http://www.gao.gov/new.items/d11421.pdf.

[141] *Id.*

[142] *Id.*

government civilian, or civilian contractor—that may conduct cyberspace operations," and the military services agreed.[143]

By design, LOAC establishes a firm link between command, the ability to lawfully launch attacks, and the liability of military commanders and individual operators for the misconduct of personnel on the battlefield.[144] The DoD recognizes that numerous parties (e.g., the designer, the operator, and the commander) play important roles in the deployment of a cyberweapon. But DoD's current official policy mandates only that "[p]ersons who authorize the use of, direct the use of, or operate autonomous and autonomous weapon systems must do so with appropriate care and in accordance with the law of war, applicable treaties, weapon system safety rules, and applicable rules of engagement (ROE)."[145] But this policy excludes cyberweapons; it also seemingly exempts designers.

A better, more robust policy must consider programmers when their code possesses enough discretion to warrant exposure to LOAC. In the case of autonomous cyberweapons, the designer performs tactical-level planning involving target acquisition before the operator even touches a computer terminal. Thus, if the program commits a war crime due solely to logic contained within its programming, the weapon's programmers must be held accountable.[146] On the other hand, where a LOAC violation stems from an operator directing an attack against an unlawful target, the programmer would be absolved of liability. Additionally, the commander or civilian supervisor, if he "knew or should have known that the autonomous weapon had been so programmed and did nothing to stop its use," would share responsibility.[147]

Certainly, if cyberweapons designers were formalized as lawful combatants, this tension and confusion would quickly dissipate. They would possess the right to

---

[143] *Id.* at 10.

[144] Corn, *supra* note 109, at 271.

[145] DoD Dir. 3000.09, *supra* note 2, para. 4b.

[146] Schmitt, *supra* note 67, at 22 (citations omitted).

[147] *Id.* The "known or should have known standard," as applied to commanders or responsible supervisors, is identical to the standard to which these persons are held vis-à-vis traditional war crimes. *See, e.g.*, William H. Parks, *Command Responsibility for War Crimes*, 62 Mil. L. Rev. 1, 94 (1973) ("Almost universally the post-World War II tribunals concluded that a commander is responsible for offenses committed within his command if the evidence establishes that he had *actual knowledge* or *should have had knowledge,* and thereafter failed to act."). This is known as the *Yamashita* standard, following In Re Yamashita, 327 U.S. 1 (1946). *See also* Michael L. Smidt, *Yamashita, Medina, and Beyond: Command Responsibility in Contemporary Military Operations*, 164 Mil. L. Rev. 155 (2000); Mark S. Martins, *"War Crimes" During Operations Other than War: Military Doctrine and Law Fifty Years After Nuremberg—And Beyond*, 149 Mil. L. Rev. 145 (1995); L.C. Green, *Command Responsibility in International Humanitarian Law*, 5 Transnat'l L. & Contemp. Probs. 319 (1995); U.S. Dep't. of Army, Field Manual 27-10, The Law of Land Warfare (July 1965) [hereinafter FM 27-10], *available at* http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm27_10.pdf.

carry out lawful attacks, including all phases of warfare—including the tactical-level planning embodied in writing decision-making algorithms. On the other hand, if these functions were carried out by a non-combatant civilian, that person forfeits POW protection and her actions could also be considered tantamount to criminal acts.[148] The urgency of the first forfeiture, contingent upon capture by a hostile force, resonates weakly: operators of cyberweapons generally sit in air conditioned office buildings or secure military compounds. The likelihood of opposing forces directly targeting and capturing American personnel is admittedly low.

But the second forfeiture, exposing civilians or contractors to criminal liability or violations of the laws of war, proves more prescient. As far as possible lawsuits go, one commentator predicts an increase in litigation and notes that historically the American government indemnified contractors from third-party liability.[149] But this defense is triggered only when contractors conform to "reasonably precise specifications," which in practice has been supplanted by requiring contractors to meet performance standards.[150] The design of cyberweapons will undoubtedly fall into the latter category, not only due to present convention, but because calling upon a weapon to achieve a certain effect (e.g., "capable of dismantling the continuous operations of the targeted electric power plant") is far easier to draft than demanding certain snippets of source code.[151]

In either case, DoD must fully define permissible roles for civilians. The Department publicly admits a growing demand for individuals versed in information technology, ready to defend against the increasing threat of defending against cyber-attacks. Further, it pledged to "catalyze U.S. scientific, academic, and economic resources to build a pool of talented civilian and military personnel to operate in cyberspace and achieve DoD objectives."[152] One initiative, the Cyber Corps program, spearheaded by the University of Tulsa, even trains undergraduates

---

[148] Brown, *supra* note 32, at 190.

[149] Bodenheimer, *supra* note 13, at 3.

[150] *Id.* (citing Boyle v. United Technologies Corp., 487 U.S. 500, 512 (1988)).

[151] *See* DARPA Agency Announcement, *supra* note 15 (showcasing a prime example of an agency announcement for a cyberweapon using performance-based requirements).

[152] U.S. Dep't. of Defense, Strategy for Operating in Cyberspace 10-11 (July 2012), *available at* http://www.fas.org/man/eprint/dod-cyber.pdf. The strategy claims further that

> DoD must make itself competitive if it is to attract technically skilled personnel to join government service for the long-term. To achieve its objectives, DoD will focus on the establishment of dynamic programs to attract talent early, and the Department will leverage the 2010 Presidential Initiative to improve federal recruitment and hiring processes. DoD will also work with the Executive Office of the President to explore strategies designed to streamline hiring practices for its cyber workforce and exchange programs to allow for "no penalty" cross-flow of cyber professionals between the public and private sectors to retain and grow innovative cyber talent."

*Id.* at 11.

in cyber-espionage; they often find careers in American government agencies.[153] When these budding cyber-warriors join DoD, United States Cyber Command (USCYBERCOM), created in 2010, trains and equips them.[154]

The same goes for delineating the ideal composition of forces dedicated to America's cyberspace forces.[155] USCYBERCOM plans to add an additional 1,000 civilian employees to the "network operations and security workforce over the next two years."[156] General William Shelton, the commander of the Air Force's Space Command, claimed in January 2013 that cyberspace is "the Wild West because you can be anywhere and do anything and be effective. All you need is an Internet connection, the right skills and a laptop and you're in the game."[157] This may be true, but DoD also needs clearer policies to ensure the activities of its programmers and operators comply with LOAC.

D. A Suggested Framework to Ensure Civilians' Protected Status

Ordinarily, this problem could be solved by relying solely upon uniformed personnel, but the services lack the required technical skills. Indeed, as demand for cyberweapons increases, military forces will undoubtedly train their uniformed men and women, but they will also rely upon civilians and hire contractors to shoulder the expanded mission. This amounts to "blurring the distinction between civilians and military personnel."[158]

For instance, Professors Brenner and Clarke propose that civilians should be "integrated" directly into the military, which also implicates the criteria required by Article 4(A)(2) of the Third Geneva Convention. Louise Doswald-Beck, formerly with the ICRC, shares this conclusion and even suggests that personnel involved in

---

[153] Ken Dilanian, *Cyber Corps Program Trains Spies for the Digital Age*, L.A. Times (Nov. 22, 2012), http://articles.latimes.com/2012/nov/22/nation/la-na-cyber-school-20121123.

[154] Feickert, *supra* note 9, at 22 ("USCYBERCOM is a sub unified command that is subordinate to USSTRATCOM. USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to defend DoD information networks and also conducts cyber space activities to enable U.S. military activities.").

[155] Wesley R. Andrues, *What U.S. Cyber Command Must Do*, Joint Forces Quarterly no. 59 at118-19 (2010), *available at* http://www.ndu.edu/press/lib/images/jfq-59/JFQ59_115-120_Andrues.pdf ("To date, no all-inclusive IO career structure has been codified, due largely to a lack of Service consensus on the extent and makeup of core IO skills and force composition. Thus, the key intent of the DoD instruction—to establish policy, definitions, and responsibilities for the force—has not yielded a decisive deliverable.").

[156] Sean Gallagher, *Air Force's Cyber Commander Says Iran Is Next Big 'Net Menace*, Ars Technica (Jan. 18, 2013), http://arstechnica.com/security/2013/01/air-forces-cyber-commander-says-iran-is-next-big-net-menace/.

[157] *Id.*

[158] Brown, *supra* note 32, at 183.

cyberwarfare wear uniforms altogether.[159] However, to qualify under this definition, a responsible officer must command every member.[160] But under any proposed plan for integration, the command relationship arrangement must be assured.[161]

Brenner and Clarke note that a recent amendment to the Uniform Code of Military Justice (UCMJ), the unitary basis of criminal law for the armed forces,[162] potentially solves this dilemma. In 2006, Congress extended its jurisdiction, in some cases, to civilians serving with the armed forces.[163] Article 2(a)(10) of the UCMJ provides that "[i]n time of declared war or contingency operation, persons serving with or accompanying an armed force in a field" are subject to military jurisdiction, and thus command authority.[164] The Office of the Secretary of Defense, in a memorandum released in 2008, elaborated upon this jurisdictional extension. For offenses committed within the United States (and violations of LOAC can be charged under the UCMJ[165]), the Secretary of Defense retains the authority to formally bring charges and court-martial civilians accompanying the forces.[166]

In short, command authority exists, provided the civilians or contractors fall under the ambit of Article 2(a)(10). Professor Geoffrey Corn argues, however, that the mere penal authority of commanders to impose some punishment may not be enough to effectively qualify a corps of civilians for combatant status—a full regime of command and control, defined by the superior-subordinate relationship, must exist.[167]

---

[159] Louise Doswald-Beck, *Computer Network Attack and the International Law of Armed Conflict*, *in* Computer Network Attack and International Law 163 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002).

[160] GC3, *supra* note 103, art. 4(A)(2).

[161] Brenner & Clarke, *supra* note 75, at 1057-74.

[162] Uniform Code of Military Justice, 10 U.S.C. §§ 801-946 (2012).

[163] *See, e.g.*, Kovach, *supra* note 93.

[164] 10 U.S.C. § 802(a)(10) (2012). Additionally, 10 U.S.C. § 101(a)(13) notes that a contingency operation is a "military operation" that "(A) is designated by the Secretary of Defense as an operation in which members of the armed forces are or may become involved in military actions, operations, or hostilities against an enemy of the United States or against an opposing military force; or (B) results in the call or order to, or retention on, active duty of members of the uniformed services . . . or any other provision of law during a war or during a national emergency declared by the President or Congress."

[165] For examples of possible charging strategies, *see* Martin N. White, *Charging War Crimes: A Primer for the Practitioner*, Army Lawyer (Feb. 2006), *available at* http://www.au.af.mil/au/awc/awcgate/law/war_crime_charging.pdf.

[166] Memorandum from the Secretary of Defense, to the Secretaries of the Military Departments, subject: UCMJ Jurisdiction over DoD Civilian Employees, DoD Contractor Personnel, and Other Persons Serving with or Accompanying the Armed Forces Overseas During Declared War and Contingency Operations (Mar. 10, 2008), *available at* http://www.justice.gov/criminal/hrsp/docs/03-10-08dod-ucmj.pdf.

[167] Corn, *supra* note 109, at 260 n.6 ("Simply subjecting a civilian augmentee to military

In order for this proposal to succeed, DoD civilians possessing the discretion to potentially commit violations of LOAC must formally be attached to the armed forces and subject to the orders of the commander holding overall responsibility for the mission. This shift basically demands formal induction into the armed forces, at least in the "reservist" capacity mentioned by Professor Schmitt in the discussion concerning Article 4(A)(1) of the Third Geneva Convention above. Qualifying civilians must be set apart from other classes of civilians who merely perform support functions. In other words, to the maximum extent possible, the corps of civilians participating in the development of autonomous cyberweapons must act, in many respects, like a paramilitary organization.[168] And they must be commanded and subject to a formal disciplinary structure, not just supervised.

Moreover, one scholar argues that only those subject to command authority should be able to exercise discretion that could result in a law of armed conflict violation.[169] Where designers translate strategic guidance to tactical-level planning in the form of decision-making algorithms, that sort of discretion already exists. And those in command are responsible for the actions of their inferiors, regardless of "whether the conflict amounts to an international armed conflict, a civil war, or an operation under the auspices of the United Nations or some other international organization."[170]

Beyond the questions raised by ordinary civilians, who might qualify for combatant status under Article 4(A)(1) of the Third Geneva Convention, contractors might instead enjoy protection under Article 4(A)(2) provided they meet the applicable criteria. However, the threshold criterion is whether the contractor possesses independence from the armed forces and the ability to conduct operations autonomously (as, for example, a private security company might, or for the purposes of this article, the contractor awarded DARPA's Plan X contract). Otherwise, without this requisite autonomy, the contractor "would be indistinguishable from Article 4(A)(1) militia and volunteer corps," and would instead function as part of the military.[171]

---

disciplinary authority would not, in the opinion of this author, transform the civilian into a 'member of the armed forces' for purposes of the LOAC. The penal authority of a military commander is only one aspect of comprehensive command and control and unit discipline over a fighting force. Rather, the complex relationship between superior and subordinate, and the relationship among all members of a military unit, produce the cohesion and discipline inherent in the concept of 'military unit.'").

[168] GC3, *supra* note 103, art. 4(A)(2).

[169] Corn, *supra* note 109, at 261.

[170] Green, *supra* note 147, at 371.

[171] Schmitt, *supra* note 99, at 528 ("In crafting Article 4, the drafters adhered to the distinction in Article 1 of the 1907 Hague Regulations between 'militia and volunteer corps forming part of the army and those which are independent'—hence, Article 4(A)(1) *and* Article 4(A)(2).").

Provided the contractor exercises independence and satisfies the remaining Article 4(A)(2) criteria—having a commander; bearing fixed, distinctive signs; carrying arms openly; and conducting operations in accordance with the laws of war—they could possibly qualify as a paramilitary organization that grants its members combatant status.[172] But while such analogies may ring true for private security companies operating in conflict zones, it seems incredibly unlikely that prospective Defense Department contractors would independently reform their organizations to give their IT department the veneer of Blackwater.

Instead, the most workable solution involves formalization and incorporation similar to that which ordinary government civilian employees participating in the design or operation of cyberweapons should receive. However, while most of those Article 4(A)(2) criteria, such as wearing distinctive clothing and conducting operations in accordance with LOAC, seem surmountable, having a "commander" proves difficult—for statutory fiscal reasons.

It is well established that only Congress itself may authorize the expenditure of public funds.[173] Contractors provide services or products in exchange for appropriated funds. As noted by the Federal Circuit, "federal expenditures would be wholly uncontrollable if Government employees could, of their own volition, enter into contracts obligating the United States."[174] In other words, while the United States possesses the authority to contract with individuals, this authority is limited, highly guarded, and heavily regulated.[175]

The Federal Acquisition Regulation (FAR)[176] provides stringent, sometimes byzantine restrictions on government procurement.[177] The FAR vests contracting authority in the head of the agency—for example, the Secretary of Defense, who may further delegate this authority.[178] Here, as applied to contractor personnel involved with the design and operation of cyberweapons, only rarely would the commanders of entities to which contractors are assigned possess the authority to contract (or, more bluntly, to tell contractors what to do). This invites some tension: telling a contractor to "fix that" or "adjust this weapon" could lead to unauthorized commitments of federal funds. Moreover, this codified break in authority between the one responsible for the contractor's conduct under the laws of war and the contractor himself strongly suggests the inapplicability of that Article 4(A)(2) criterion.

---

[172] GC3, *supra* note 103, art. 4(A)(2).

[173] United States v. MacCollom, 426 U.S. 317 (1976).

[174] City of El Centro v. United States, 922 F.2d 816, 820 (Fed. Cir. 1990).

[175] United States v. Tingey, 30 U.S. (5 Pet.) 115 (1831).

[176] Gen. Servs. Admin. et al., Federal Acquisition Reg. [hereinafter FAR].

[177] The Department of Defense has its own supplement, the Defense Federal Acquisition Regulation Supplement. U.S. Dep't of Def., Defense Federal Acquisition Reg. Supp. [hereinafter DFARS].

[178] FAR, *supra* note 177, § 1.601(a); DFARS, *supra* note 177, § 202.101.

Certainly any conflict between violations of the Antideficiency Act, which prohibits the practices described above, and preventing violations of the laws of war must be resolved in favor of the latter.[179] But as it stands, the existence of command authority for contractor personnel involved with the design and operation of cyberweapons depends principally upon whether they fall under military jurisdiction, presumably via the UCMJ. Because contractors are beholden to contracting officers and not commanders, their link to the disciplinary structures required by LOAC to qualify as possible combatants is far more tenuous than civilians'.

In an ideal world, DoD would rely solely upon in-house members to design offensive cyberweapons. Given the current composition of American forces, however, this will likely prove unfeasible. For qualifying contractor personnel, exposure to the jurisdiction of the UCMJ, explicitly recognized in the contract vehicle, could lead to protection under the Geneva Conventions as a lawful combatant. Other safeguards should be employed, such as defining an explicit command and control relationship. The Department could consider investing the commander having responsibility for the overall mission with a warrant to obligate appropriated funds. Regarding criminal prosecution or the logistics of indemnification for possible lawsuits, the government, as it has in the past, may opt instead to shield defense contractors from financial liability arising from lawsuits.[180]

In sum, if DoD plans to rely upon the expertise of civilians and contractors (and all signs point to this practice continuing), their status must be clarified. Specific regulatory changes must clarify the flow of command responsibility and guarantee individuals associated with the deployment of autonomous cyberweapons the protections of LOAC.

Formalizing the chain of command responsibility reduces the risk that civilians and contractor personnel affiliated with cyberweapons programs would be deemed "unlawful combatants." Where a healthy portion of a weapon's discretion depends entirely upon source code written by programmers long before a conflict begins, this risk must be addressed. Applying these principles ensures American compliance with LOAC, an important effort in its own right; it also guarantees that those interested in contributing to the country's defense are not deterred or dissuaded by the risk of litigation. In the end, any sustainable plan for resolving this problem must ensure that U.S. civilians involved in the creation of autonomous cyberweapons qualify as lawful combatants.[181]

---

[179] The Antideficiency Act refers to several statutes that allow for administrative and criminal sanctions in response to the unlawful obligation and expenditure of appropriated funds. 31 U.S.C. §§ 1341-42; 1350-51; 1511-19 (2012).

[180] *See, e.g.*, Hercules, Inc. v. United States, 516 U.S. 417, 420-22 (holding that the risk of loss for injuries perpetuated by the Agent Orange chemicals fell upon the manufacturers of the product rather than the government).

[181] Some have called for the creation of a standing branch of the military dedicated to prosecuting cyberwarfare. That may be inevitable, and it may even be advisable, but change takes time. *See,*

## III. THE LEGAL ROLE: REVIEWING CYBERWEAPONS FOR COMPLIANCE WITH THE LAWS OF WAR

The United States agrees that significant modifications to weapons systems require competent legal review in order to address the concerns described above. In order to pass muster, such a review must generally ensure the weapon's decision-making algorithms concerning targeting, or its built-in rules of engagement (ROE),[182] enable "even computers lacking background information . . . to avoid harming noncombatants and friendly personnel."[183] Doing so maintains the LOAC's fundamental principles of distinction and proportionality. A coherent analysis should also explore, based on the weapon's level of autonomy, potential liability for its designers and operators. General Keith Alexander, former director of the National Security Agency and former commander of USCYBERCOM, has publicly called for ROE focused on cyberweapons. Currently, there are none.[184]

Instead, the White House possesses broad authority to marshal its cyberweapons against foes, reserving the right to "order a pre-emptive strike if the United States detects credible evidence of a major digital attack looming from abroad."[185] According to the current framework, DoD offensive action remains contingent upon direct presidential approval.[186] While this arguably raises other policy concerns, the fact that streamlined engagement processes exist, but well-defined restrictions on their use by military and intelligence agencies do not, is troubling.

The proposed solution to this entire dilemma, exemplified by DARPA's Plan X system, which manages cyberwarfare by giving its operators "playbooks"

---

*e.g.*, Natasha Solce, *The Battlefield of Cyberspace: The Inevitable New Military Branch—The Cyber Force*, 18 Alb. L.J. Sci. & Tech. 293 (2008).

[182] In conventional terms, rules of engagement (ROE) dictate "who can shoot at what, with which weapons, when, and where." Martins, *supra* note 147, at 174 (quoting Fred Green, *An Address to the American Society of International Law, on the Subject of Implementing Limitations on the Use of Force: The Doctrine of Proportionality and Necessity* (1992) (using this informal definition of ROE), reprinted in 86 Am. Soc'y Int'l L. Proc. 39, 62-67 (1992)). In cyberspace, ROE govern essentially the same things, substituting "shoot" for "target," albeit with non-kinetic systems designed to degrade, disrupt, or destroy of an adversary's networks or critical infrastructure.

[183] Marcus Schulzke, *Robots as Weapons in Just Wars*, 24 Phil. & Tech. 293, 300 (2011).

[184] Ellen Nakashima, *Pentagon Proposes More Robust Role for Its Cyber-Specialists*, Wash. Post (Aug. 9, 2012), http://www.washingtonpost.com/world/national-security/pentagon-proposes-more-robust-role-for-its-cyber-specialists/2012/08/09/1e3478ca-db15-11e1-9745-d9ae6098d493_story.html.

[185] David E. Sanger and Thom Shanker, *Broad Powers Seen for Obama in Cyberstrikes*, N.Y. Times (Feb. 3, 2013), http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html?pagewanted=all&_r=2&.

[186] Sean Gallagher, *President Given "Broad Authority" to Order Cyber Attacks*, Ars Technica (Feb. 4, 2013), http://arstechnica.com/tech-policy/2013/02/president-given-broad-authority-to-order-cyber-attacks/.

from which to select attacks, asks designers to build ROE directly into the software itself. The agency announcement states:

> Enforcing Rules of Engagement (ROE). Plans should be constructed to programmatically limit and enforce operator options and actions, according to a commander's specified ROEs. By integrating ROEs directly into a plan, they can be seamlessly integrated into a mission script during the script synthesis process. This allows formal analysis techniques to mathematically prove the limitations of an operator's ability to negatively affect the mission and operate without authority.[187]

Thus, the code polices itself. It relies upon electronic governors that restrict the weapon's employment. However, software malfunctions. Bugs could lead to those unintended consequences DoD seeks to avert. Moreover, even preplanned use cases must be thoroughly studied to guard against both "collateral computer damage" and real, physical collateral damage to noncombatants. Cyberweapons leverage new technologies; they are not merely newer ways to deliver explosive munitions. In many aspects, conventional weapons are much easier to assess. As one scholar notes, while most of us "do not know how to fly airplanes . . . we know about the effects of aerial bombing."[188] A short trip to Wikipedia readily explains simple concepts like blast radius, and maps (or Google Earth) instantaneously display schools, hospitals, and residential areas.

This Article asserts that reviewing a cyberweapon necessarily implicates both: (1) a thorough technical review of a weapon's source code; and (2) consequence management through studying the potential effects of employment. These twin aims are complementary, and legal analysis pervades both threads. Still, some attorneys and policy wonks, such as Stewart Baker, acknowledge the risk but pessimistically forecast the success of these analyses:

> In that climate [discussing the application of airpower during the Second World War], all it took was a single error to break the legal limits irreparably. And error was inevitable. Bombs dropped by desperate pilots under fire go astray. But so do cyberweapons. Stuxnet infected thousands of networks as it searched blindly for Natanz. The infections lasted far longer than intended. Should we expect fewer errors from code drafted in the heat of battle and flung at hazard toward the enemy? Of course not. But the lesson for the

[187] DARPA Agency Announcement, *supra* note 15, at 16.

[188] Philip Spoerri, *Round Table on New Weapon Technologies—Conclusions*, Int'l Comm. of the Red Cross (Sept. 13, 2011), http://www.icrc.org/eng/resources/documents/statement/new-weapon-technologies-statement-2011-09-13.htm.

> lawyers and the diplomats is stark: Their effort to impose limits on cyberwar is almost certainly doomed.[189]

Despite these difficulties, DoD policy nevertheless charges its lawyers with ensuring all its weapons comply with LOAC.[190] This policy requires weapons acquisition and procurement to be "consistent with all applicable domestic law and treaties and international agreements . . . , customary international law, and the law of armed conflict."[191] And qualified attorneys must conduct these legal reviews.[192] Further, in the specific case of cyberweapons, the Air Force has since promulgated a directive extending and implementing DoD policy. The other services have not yet done so, but the general, high-level nature of the Air Force policy, compounded by its brevity (it consists only of seven pages) and lack of service-specific elements, lays the foundation for other directives from the rest of the armed forces.

The relevant Air Force Instruction mandates the following process for requesting a legal review for a new cyberweapon:

> 2.1. Upon cognizant legal authority's request, Air Force personnel will provide the following information, so that a judge advocate, or General Counsel in the instance of a special access program, may complete the reviews required by this Instruction:
>
> 2.1.1. A *general description* of the weapon or cyber capability submitted for legal review.
>
> 2.1.2. Statements of *intended use* (such as types of targets) or concept of operations.
>
> 2.1.3. The *reasonably anticipated effects* of employment, to include all tests, computer modeling, laboratory studies, and other technical analysis and results that contribute to the assessment of reasonably anticipated effects.[193]

In short, the reviewing attorney only sees the reasonably anticipated effects of a weapon's intended use: a broad, general sketch without reference to the code itself. Admittedly, doing otherwise would be practically impossible. The DoD

---

[189] Baker & Dunlap, *supra* note 31.

[190] Gallagher, *supra* note 186 ("So far, the only software-based attack that has been attributed to the United States (though never officially acknowledged by the U.S. government) has been the Stuxnet virus, which was reportedly codeveloped with Israeli intelligence to disable production equipment in an Iranian nuclear facility. Other sophisticated malware attacks, such as Flame, Duqu, and Gauss have not been definitively tied to the United States, but analysts at Kaspersky Labs and other antivirus and network security firms have described them as 'state-sponsored.'").

[191] U.S. Dep't. of Def., Dir. 5000.01, The Defense Acquisition System para. E1.1.15 (Nov. 20, 2007), *available at* http://www.dtic.mil/whs/directives/corres/pdf/500001p.pdf.

[192] *Id.*

[193] AFI 51-402, *supra* note 24, para 2.1 (emphasis added).

predicts that programs' lines of code will increase in number, effectively blocking any efforts to test programs exhaustively; and that testing will thus require "analytical tools that work with realistic assumptions, including approaches to bound uncertainty caused by learning/adaptation."[194] The Air Force Instruction recognizes these limitations. It appropriately authorizes its attorneys to request relevant technical analyses and documents that shed light upon the cyberweapon's possible effects.

But the Instruction seemingly fails to envision discussions between counsel for the Air Force and the designers of the cyberweapon. Nor does it consider that the reviewing lawyer will only occasionally enjoy a thorough background in the implicated subject. For example, as of February 2013, of the twelve American attorneys currently assigned to the Air Force Operations and International Law Directorate, the entity charged with taking the lead on reviewing cyberweapons, two possessed engineering degrees; one had previous experience with USCYBERCOM; and others were trained extensively in international and comparative law—this is a good thing.

But it could be better. This Article submits that, with the advent of such novel technology, attorneys both deserve and require training to grasp its complexities. The governing Air Force Instruction itself demands that lawyers assess:

> 3.1.1. Whether there is a specific rule of law, whether by treaty obligation of the United States or accepted by the United States as customary international law, prohibiting or restricting the use of the weapon or cyber capability in question.
> 3.1.2. If there is no express prohibition, the following questions are considered:
>
> > 3.1.2.1. Whether the weapon or cyber capability is calculated to cause superfluous injury, in violation of Article 23(e) of the Annex to Hague Convention IV; and
> > 3.1.2.2. Whether the weapon or cyber capability is capable of being directed against a specific military objective and, if not, is of a nature to cause an effect on military objectives and civilians or civilian objects without distinction.[195]

The legal review process correctly requires attorneys to assess a weapon's compliance with the principle of distinction. But in the case of cyberweapons, the *sine qua non* of compliance (and noncompliance) is the programming itself. The rest of the Defense Department seemingly recognizes this truism. The DoD requires its procurement officers to structure cyberweapons acquisitions "to acquire full government ownership of . . . software, including source code and all documentation required to enable a third party upgrade to the functional capability."[196]

---

[194] DoD Autonomy Report, *supra* note 90, at 91.

[195] AFI 51-402, *supra* note 24, para. 3.1.1-3.1.2.

[196] DoD Autonomy Report, *supra* note 90, at 60-61. The Report goes on to note that "[m]ost of

So far, the Instruction, signed and approved by the Judge Advocate General of the Air Force (who, as noted above, expressed concerns in 2010 regarding the participation of civilians in cyber-attacks) seems reasonable.[197] But the policy concludes by stating that any possible issues with a weapon's employment, operation, or targeting fall outside the legal review process altogether. That analysis is left instead to the operations law attorney advising the commander having responsibility for a given cyber-attack.[198] The original legal review could conceivably address a myriad of concerns, ranging from liability issues stemming from the participation of civilian designers to identifying questionable use cases that could impact collateral damage assessments. But this scarcely benefits the attorney standing beside the operator's terminal.

Professor Dunlap, himself the former Air Force Deputy Judge Advocate General, argues for a "legal requirement to assess the impact on civilians and civilian objects before launching a cyberattack."[199] This Article agrees. But without knowing (to some degree) the internal workings of the cyberweapon, the attorney providing counsel to the operator suffers real disadvantages. So does the effort of both to prevent LOAC violations.

This Article proposes two initiatives to mitigate these risks. First, DoD must codify a bridge between designers and operators, including between the reviewing attorney and the attorney providing on-demand counsel about targeting. Whatever tools, tests, and correspondence the reviewing attorney viewed must be passed along to the advising attorney. This includes, as the Air Force Instruction requires, the reasonably anticipated effects of the weapon's employment. Second, both attorneys must be trained on the cyberweapon's use and operational capacity. Unlike the very basics of dropping munitions, something quickly grasped by laypersons, the military should take a progressive approach and recognize that all personnel involved in the deployment of cyberweapons need specialized training. Currently, logistical aspects, such as formalized training, remain unsettled. General Shelton recently announced new personnel hires at 24th Air Force, which supports USCYBERCOM: about 80 percent will be military, but the services have "yet to decide how the new workers will be recruited and what qualifications will be needed."[200]

---

the unmanned systems currently in the DoD inventory consist of contractor-proprietary, on-board autonomy and control software, with often closed, proprietary operator control systems (OCS). Under such circumstances, the government is constrained to returning to the development contractor for all enhancements, often slowing the pace of innovation and evolution of operational capability." *Id.* at 11. In other words, much like being beholden to Microsoft for upgrades of the Windows operating system, DoD is equally reliant upon contractors for OCS.

[197] *See supra* II(A).

[198] AFI 51-402, *supra* note 24, para. 3.3.

[199] Baker & Dunlap, *supra* note 31.

[200] Brian Everstine, *AF to Add More than 1,000 Cyber Workers*, Army Times (Feb. 4, 2013), http://www.armytimes.com/article/20130131/NEWS/301310332/AF-add-more-than-1-000-cyber-workers.

Expanded personnel numbers require a concomitant improvement of the weapons evaluation process. Doing otherwise invites risk, but continuing with the status quo adds little value to commanders concerned with mission achievement. Decision-makers throughout the DoD should push hard for these advancements, including the attorneys peppered throughout the Department, who possess a vested and legitimate interest in perfecting their craft. In order to do so, education and training are needed, perhaps in the form of specialized "tracks" that affirm the growing importance of cyberwarfare. Senior leaders and flag officers recognize the need. In fact, the Chief Information Officer of the Air Force called for an evaluation of the service's ability to support USCYBERCOM.[201] The Department's General Counsel and its Judge Advocates General should do the same.

## IV. CONCLUSION

According to security experts, the Stuxnet virus, unofficially attributed to the United States and Israel, "attacked and destroyed only specific gas centrifuges used to highly enrich uranium, operating at a specific speed . . . unique to the machines operating at the Natanz facility" in Iran.[202] Findings from security experts confirmed this; the weapon, with its built-in ROE to uphold the LOAC principle of distinction, initially proved harmless elsewhere—until a programming bug allegedly allowed the worm to infect other computers via the Internet.[203] Even more recently, in May 2013, in a story whose elements are becoming increasingly more common, attackers targeted the computers of American government employees involved in nuclear weapons research to install malware.[204]

Programming errors happen, and software can be defective by design, a risk compounded by increasing degrees of autonomy, which necessarily invokes more lines of code, more contingencies, and more decisions taken at the machine level. Or, software could work exactly as intended and place our nation's critical infrastructure at risk. In either case, while the laws of war are capable of respecting humanitarian values during the use of autonomous weapons system, respecting these principles requires effort.[205]

---

[201] *Id.*

[202] John Richardson, *Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield*, 29 J. Marshall J. Computer & Info. L. 1, 21 (2011).

[203] Jeffries, *supra* note 14. Fortunately, identifying the programming error could prove entirely possible. In 2012, weapon's source code was leaked onto the Internet, allowing it to be studied and repurposed for alternative uses. Thomas Ricker, *Stuxnet Source Code Could Open a Pandora's Box of Cyberwarfare*, The Verge (Mar. 5, 2012), http://www.theverge.com/2012/3/5/2845848/stuxnet-source-code-opens-a-pandoras-box-of-cyberwarfare.

[204] Dan Goodin, *Internet Explorer Zero-Day Exploit Targets Nuclear Weapons Researchers*, Ars Technica (May 3, 2013), http://arstechnica.com/security/2013/05/internet-explorer-zero-day-exploit-targets-nuclear-weapons-researchers/.

[205] Schmitt, *supra* note 67, at 23.

This effort calls for additional training; a recognition that cyberwarfare undoubtedly will occupy a larger portion of the Department of Defense's strategy in the future; and an understanding that personnel charged with supporting the cyber-mission, both uniformed military members and civilian employees, should operate within a framework designed to avert violations. This Article has shown that the United States has essentially engaged in a "cart-before-horse" approach to cyberwarfare, planning new methods of attack without establishing fundamental, bedrock procedures to ensure compliance with the laws of war. President Obama recently identified cyber-security as one of his concerns, issuing an Executive Order calling for bolstering the nation's defenses.[206] Undeniably, identifying and neutralizing threats is part of a robust defensive posture, meaning that DoD should take the lead in devising ROE and weapons review processes to work in harmony with other cyberspace initiatives.

Failing to act could impact attaining military commanders' practical and strategic goals. Confusion over the permissible scope of novel technologies' employment—along with practically unavoidable confusion over how the technology works—hampers military efforts. In the United States, commanders "tend to be quite wary of innovative but relatively untested means of warfare, particularly when the rules of conduct are so arcane and ill-defined."[207] They deserve better. More importantly, so do the civilians facing a cyberweapon's possible "unintended consequences."

[206] Exec. Order No. 13636, 78 Fed. Reg. 11739 (Feb. 19, 2013).

[207] Brown, *supra* note 32, at 183.

## INFORMATION FOR CONTRIBUTORS

*The Air Force Law Review* publishes articles, notes, comments, and book reviews. The Editorial Board encourages readers to submit manuscripts on any area of law or legal practice that may be of interest to judge advocates and military lawyers. Because the *Law Review* is a publication of The Judge Advocate General's Corps, USAF, Air Force judge advocates and civilian attorneys are particularly encouraged to contribute. Authors are invited to submit scholarly, timely, and well-written articles for consideration by the Editorial Board. The *Law Review* does not pay authors any compensation for items selected for publication.

**Manuscript Review**. Members of the Editorial Board review all manuscripts to determine suitability for publication in light of space and editorial limitations. Manuscripts selected for publication undergo an editorial and technical review, as well as a policy and security clearance as required. The Editor will make necessary revisions or deletions without prior permission of, or coordination with the author. Authors are responsible for the accuracy of all material submitted, including citations and other references. The *Law Review* generally does not publish material committed for publication in other journals. In lieu of reprints, authors are provided two copies of the issue containing their work.

**Manuscript Form**. Manuscripts may be submitted by disc or electronic mail in Microsoft Word format. Please contact the Editor at (334) 953-2802 for submission guidelines or contact the Editor at AFLOA.AFJAGS@us.af.mil and provide your electronic contact information. Authors should retain backup copies of all submissions. Footnotes must follow the format prescribed by A Uniform System of Citation (19th ed. 2010). Include appropriate biographical data concerning the author(s), such as rank, position, duty assignment, educational background, and bar affiliations. The Editorial Board will consider manuscripts of any length, but articles selected for publication are generally less than 60 pages of text. The *Law Review* does not return unpublished manuscripts.

**Distribution**. *The Air Force Law Review* is distributed to Air Force judge advocates. In addition, it reaches other military services, law schools, bar associations, international organizations, foreign governments, federal and state agencies, and civilian lawyers.


THE JUDGE ADVOCATE GENERAL'S SCHOOL
UNITED STATES AIR FORCE