Penn State Journal of Law & International Affairs

Volume 5
Issue 1 *War in the 21st Century and Collected Works*

April 2017

War in the 21st Century and Collected Works

ISSN: 2168-7951

Penn State
Journal of Law & International Affairs

2016 – 2017

Penn State
Journal of Law & International Affairs

2017 VOLUME 5 NO. 1

THE CYBER LONGBOW & OTHER INFORMATION STRATEGIES: U.S. NATIONAL SECURITY AND CYBERSPACE

*Gary D. Brown**

* Gary D. Brown is a retired U.S. Air Force Judge Advocate. He served as U.S. Cyber Command's first senior legal counsel.

TABLE OF CONTENTS

I. INTRODUCTION

The U.S. is struggling to effectively contest its adversaries in cyberspace. It would seem natural for the U.S. to be the leader in every aspect of internet operations, after all, the internet was invented in the U.S., and the U.S. is dominant in many areas. However, there are regions of cyberspace in which the U.S. is not the leader, perhaps because of a misapprehension about the nature of cyberspace.[1]

This paper will provide a definition of cyberspace suitable for national security strategy discussions and address how the U.S. should approach cyberspace operations to engage its adversaries in the most effective manner. Historically, the U.S. has been a champion at leveraging soft power. Cyberspace has become an essential way to increase the reach and penetration of soft power, yet the U.S. appears on some levels to be losing in cyberspace to non-state groups like ISIS and to other State actors such as Russia.

This paper suggests that it would be more effective to think of cyberspace as a combination of infrastructure (the internet) and the information and ideas that move across the infrastructure (the ideosphere, as defined below). This model of cyberspace helps increase the emphasis on engaging with the actors and information using the internet in ways counter to U.S. national interests.

II. BACKGROUND

Cyberspace is an unprecedented national security challenge. It doesn't align with standard U.S. government organizational constructs, which are generally either geographic or defined by specific functionality. Although it is hosted on physical infrastructure that has a physical location, it's often not helpful to think of cyberspace in geographic terms. Additionally, it's not straightforward to characterize it functionally because cyber capabilities support every

[1] At least one author rejects the notion that cyberspace can even have a nature. This may reflect the definitional problem discussed below. *See* Lawrence Lessig, *Code and Other Laws of Cyberspace (1999).*

agency and activity, and enable adversary activities, as well as being the primary focus of some adversary missions.

U.S. strategy seems to put less emphasis to acting on information, rather, focusing on the physical elements of cyberspace.[2] Concentrating on the hardware and operating systems – basically the internet – rather than other elements of cyberspace requires confronting specific operational issues. The internet is, well, the internet.

Disabling or destroying hardware in one location may have transnational effects. It can raise sovereignty concerns for allies and others, and restrict the ability of the U.S. to operate, in addition to compromising intelligence equities. Perhaps most vexing though, disabling or destroying hardware raises questions of how to attribute those activities to individual actors. Engaging on *content* rather than *infrastructure* can limit these issues. To some extent the U.S. has begun to realize this, undertaking at least some discussion about engaging ISIS on both its ability to use the internet to communicate, and about changing the communications to alter the message.[3]

Infrastructure-focused strategy also represents a lost opportunity. Cyber operations aren't a particularly good method for asserting national interests directly because of the ancillary effects set out above, and because they tend to be packets of boutique capabilities that don't easily translate to large-scale operations. However, cyberspace is an ideal medium for the exercise of soft power.[4] Spreading ideals of freedom of speech, economic principles, and democratically-driven culture, for example, supports U.S. national security interests. As noted below, U.S. adversaries have

---

[2] *Infra.*

[3] Sanger, *U.S. Cyberattacks Target ISIS in a New Line of Combat*, N.Y. TIMES (Apr. 24, 2016), http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news&_r=1.

[4] Soft power is the ability to get what you want through attraction and persuasion rather than coercion or payments. It arises from the attractiveness of a country's culture, political ideals, and policies. Joseph S. Nye, Jr., *Soft Power* (2004) [*hereinafter* "Nye"], pp. 5-8.

been more effective at using this aspect of cyber power to maximize their interests, which often run contrary to those of the U.S. The U.S. should do more to close this divide.

III. RIVAL APPROACHES TO CYBERSPACE

Although the U.S. is skilled in cyber activity, its focus has been on espionage and, to a lesser extent, on military activity aimed at disrupting or damaging internet infrastructure. Focusing on cyber infrastructure for non-intelligence operations has placed the U.S. behind some of its rivals in important aspects of cyberspace. Set out below are three examples of approaches to the strategic use of cyberspace that largely focus on the content rather than the infrastructure, along with suggestions regarding how the U.S. might glean lessons from each.

A. China

The modern Chinese economy was built on commercial espionage.[5] The Chinese government has even gone so far as to formalize the strategy of stealing intellectual property to advance its economy, developing a branch of the PLA, Unit 61398, dedicated to cyber espionage. By stealing industrial secrets to advance its economic might, China is following a strategy modeled in the early days of the U.S. The U.S. has protested, but it is hard to ignore the historical irony of the situation. It was national policy in the early days of the American republic to acquire European technology by any means available, a policy that resulted in the U.S. emerging as the world's industrial leader.[6] For example, in 1789 Samuel Slater emigrated to the U.S., bringing with him an intimate knowledge of the Arkwright spinning frames that had transformed textile

[5] Joshua Philipp, *Hacking and Espionage Fuel China's Growth*, EPOCH TIMES (Sept. 10, 2015), http://www.theepochtimes.com/n3/1737917-investigative-report-china-theft-incorporated/.

[6] Doron Ben-Atar, *Trade Secrets: Intellectual Piracy and the Origins of American Industrial Power* (2004); Alexander Hamilton, *Report on the Subject of Manufactures* (Dec. 5, 1791), http://www.constitution.org/ah/rpt_manufactures.pdf.

production in England. Using this knowledge, Slater set up the first water-powered textile mill in the U.S. Two decades later, the American businessman Francis Cabot Lowell talked his way into a number of British mills, and memorized the plans for the hi-tech Cartwright power loom.[7]

The U.S. and China agreed in 2015 not to engage in commercial espionage against each other, but there is doubt China will uphold its end of the bargain. If China violates the agreement the U.S. government may respond with economic and political action, but there is little that can be done by the U.S. to directly prevent Chinese commercial espionage. Attempts to defend against espionage have been less than completely successful. The U.S. government could respond in kind, stealing intellectual property and other commercial information from China through cyberspace – although U.S. industry is generally advanced compared to Chinese industry – so that course of action provides little gain.

For the U.S., the closest effective equivalent to Chinese action might be to remove the barriers for private citizens to strike back with cyber means as a response to being victimized by this type of action. Often called "hacking back," many companies have expressed frustration with ineffective government action in the area, and noted a willingness to use their own cyber expertise to retrieve stolen data, render it unusable, or simply to punish perpetrators by disrupting their networks. Government officials consistently note the dangers in this type of action.[8] If the U.S. decided to change course and allow self-help activity, it would have to consider amending several statutes prohibiting unauthorized access to both computers and data, at rest and in transit.[9] However, there seems to be little

---

[7] James Surowiecki, *Spy vs. Spy*, THE NEW YORKER (Jun. 9 & 16, 2014), http://www.newyorker.com/magazine/2014/06/09/spy-vs-spy-3.

[8] Craig Timberg, Ellen Nakashima & Danielle Douglas-Gabriel, *Cyberattacks trigger talk of 'hacking back*,' WASH. POST (Oct. 9, 2014), https://www.washingtonpost.com/business/technology/cyberattacks-trigger-talk-of-hacking-back/2014/10/09/6f0b7a24-4f02-11e4-8c24-487e92bc997b_story.html.

[9] These statutes include the *Computer Fraud & Abuse Act (CFAA)*, 18 U.S.C. §1030; the *Electronic Communications Privacy Act*, 18 U.S.C. §§ 2510-2521 and the *Stored Communications Act*, 18 U.S.C. §2701. CFAA, in particular, is considered by

appetite for this in Washington, and the U.S. has aggressively pursued criminal action for what might be seen as relatively minor violations of computer security statutes.[10]

B. ISIS

A non-state actor that has been active in cyberspace is ISIS.[11] ISIS has been successful at using social media to promote its message of violence and recruit members. Al Hayat, ISIS' media department, has released carefully choreographed, ideology-focused videos that have been called "Jihadi infomercials."[12] These videos present a message encouraging would-be Jihadists and foreign fighters to answer the call of duty. The videos feature foreign fighters appealing to their brothers to reject Western values and join the fight. This message provides a strong moral pull, appealing to the estranged and isolated, particularly in Western Europe and in the U.S.

ISIS spreads its message using a variety of social media, the most popular being Twitter and web forums. As ISIS advanced in its territorial acquisitions, it posted pictures of hundreds of massacred Iraqi soldiers on Twitter. The photos inspired horror and fear, which appeared to be the intended result. ISIS videos of beheadings and executions have been posted for maximum visibility. In a YouTube video uploaded in August of 2014 an Iraqi police chief was beheaded. His head was placed on his legs, and ISIS tweeted the picture with the words, "This is our football, it's made of skin." The photo included the hashtag #WorldCup, causing it to pop up in the news

---

some to be overly broad. *See* Electronic Frontier Foundation, https://www.eff.org/issues/cfaa.

[10] Mark Jaycox & Lee Tien, *Obama's Computer Security Solution is a Mishmash of Old, Outdated Policy Solutions*, ELECTRONIC FRONTIER FOUNDATION (Jan. 16, 2015), https://www.eff.org/deeplinks/2015/01/obamas-computer-security-solution-mish-mash-old-outdated-policy-solutions; Doe, *FBI raids dental software researcher who discovered private patient data on public server*, DAILY DOT (May 27, 2016), http://www.dailydot.com/politics/justin-shafer-fbi-raid/.

[11] The Islamic State in Iraq and Syria (ISIS) is also referred to as IS, ISIL, and Daesh.

[12] Jesse Singal, *Why ISIS Is So Terrifyingly Effective at Seducing New Recruits*, N.Y. MAGAZINE (Aug. 18, 2014), http://nymag.com/scienceofus/2014/08/how-isis-seduces-new-recruits.html.

feeds of those following the hugely-popular soccer tournament in Brazil, ensuring millions of views.[13] ISIS also has foreign recruits use their personal Facebook and Twitter pages to report positive experiences about the movement, posting pictures of themselves apparently living wealthily in extravagant houses, showing the material upside to joining ISIS.[14]

The U.S. has tried to engage on social media, but at least with publicly disclosed programs, it has generated more embarrassment than success.[15] As a nation, the U.S. has generally been good at using soft power, even if it most often has been a happy byproduct of American business success rather than a planned government activity. During the Cold War, for example, East Germans were able to listen to American punk rock and dissident announcements on *Radio Glasnost*, which was run by private citizens.[16] This was an example of combining the natural attractiveness of Western culture with the power of private citizens to tailor the narrative to suit U.S. national security goals.

---

[13] Tomlinson & White, *This is our football, it's made of skin #World Cup: After posting sickening beheading video of Iraqi policeman, ISIS boast of slaughtering 1,700 soldiers*, DAILY MAIL (Jun. 13, 2014), http://www.dailymail.co.uk/news/article-2656905/ISIS-jihadists-seize-two-towns-bear-Baghdad-U-S-tanks-helicopters-stolen-fleeing-western-trained-Iraqi-forces.html.

[14] Deborah Richards, *The Twitter jihad: ISIS insurgents in Iraq, Syria using social media to recruit fighters, promote violence*, AUSTRALIA BROADCASTING CORPORATION (Jun. 20, 2014), http://www.abc.net.au/news/2014-06-20/isis-using-social-media-to-recruit-fighters-promote-violence /5540474.

[15] Such as trumpeting the decision to deploy more U.S. troops to Iraq when that is one of the primary concerns of Muslims in the region. Elizabeth Cohen & Debra Goldschmidt, *Ex-terrorist explains how to fight ISIS online*, CNN (Dec. 21, 2015), http://www.cnn.com/2015/12/18/health/al-quaeda-recruiter-fight-isis-online/.

[16] Esme Nicholson, *The Cold War Broadcast That Gave East German Dissidents a Voice*, NPR (Nov. 8, 2014), http://www.npr.org/sections/parallels/2014/11/08/361160675/the-cold-war-broadcast-that-gave-east-german-dissidents-a-voice. Radio and television from West Germany was quite effective at educating East German audiences on the benefits of the non-Communist world. Esther von Richthofen, *Bringing Culture to the Masses: Control, Compromise and Participation in the GDR* (2009), p. 103.

The diverse population of the U.S., the production and international distribution of films and television programs, American domination in the music and sports scenes, and the availability of U.S. higher education to foreigners have all helped build an impressive machine for the U.S. to wield soft power.[17] Although this may not translate directly into advancing U.S. national interests, it does show the potential for spreading U.S.-based information effectively. This attraction to popular cultural has helped the U.S. achieve important foreign policy goals, such as reconstruction after WWII and victory in the Cold War.[18]

Unfortunately, the relative ability of the U.S. to project soft power seems to have diminished in the past several years. The U.S. has reduced its credibility in the Middle East by engaging in multiple conflicts there and demonstrating little cultural understanding.[19] The internet-enabled lower barrier to entry for news channels and information distribution has increased competition for the attention of the masses, and decreased the ease with which the U.S. can project its values. Official outlets in other States are more trusted by foreign countries, while U.S. official outlets are less trusted abroad than unofficial U.S. outlets.

To regain its soft power mojo, the U.S. must evolve, learning to use information to its advantage. It's easy to see, for example, how some stories could present a favorable contrast between the adversary's cause and Western values, e.g., reportage on ISIS killing male European jihadists who arrive in theater, and subjecting females who arrive to sexual slavery.[20] There is some hope on this front, as

---

[17] Nye, *supra* FN. 4, at Chap. 2.

[18] Nye, *supra* FN. 4, at 49-53.

[19] President George W. Bush's announcement of the "war on terror" and call for democratization of the Muslim world, for example, failed to engage with the local population and damaged U.S. soft power reserves. Nye, "The Future of Soft Power in U.S. Foreign Policy," in *Soft Power and US Foreign Policy* (2010), pp. 4-7.

[20] Nadette de Visser, *ISIS Eats Its Own, Torturing and Executing Dutch Jihadists. Or Did It?*, DAILY BEAST (1 Mar. 2016), http://www.thedailybeast.com/articles/2016/03/01/isis-eats-its-own-torturing-and-executing-dutch-jihadists-or-did-it.html; Sam Webb, ""A living hell': The grim fate that awaits British teenage girls

the U.S. Secretary of State met with Hollywood executives to discuss the impact on groups like ISIS of how the U.S. is portrayed in movies.[21]

In the absence of an effective U.S. government response to terrorist successes in cyberspace, and under pressure to do *something*, private companies have begun to step up their game. Notably, Google has developed a capability to redirect searches for terrorist information to pre-existing anti-terrorist material on YouTube.[22] It's too early to determine how effective the program will be.

This issue remains on the radar of strategic thinkers in the U.S. government, as well. Recently, the State Department began a new campaign to help slow recruitment efforts from extremist groups like ISIS. For example, under the new campaign, the U.S. has been shifting away from directly sending messages to potential ISIS recruits through the Center for Strategic Counterterrorism Communications (CSCC), as it proved to be ineffective.[23] The CSCC approach was ultimately abandoned after being reviewed by a team comprised of non-governmental individuals. The reviewers undoubtedly observed that it wasn't very effective to counter an organization that operates under the notion that Western governments are illegitimate with official statements from one of

believed to be joining ISIS," *Mirror* (Feb. 21, 2015), http://www.mirror.co.uk/news/uk-news/a-living-hell-grim-fate-5203372.

[21] Ryan Faughnder, *John Kerry meets with Hollywood studio executives to talk Islamic State*, L.A. TIMES (Feb. 16, 2016), http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-john-kerry-hollywood-isis-20160216-story.html.

[22] Jack Detsch, *How Google aims to disrupt the Islamic State propaganda machine*, PASSCODE (Sept. 7, 2016), http://www.csmonitor.com/World/Passcode/2016/0907/How-Google-aims-to-disrupt-the-Islamic-State-propaganda-machine?cmpid=ema:nws:Daily%2520Newsletter%2520%2809-07-2016%29&utm_source=Sailthru&utm_medium=email&utm_campaign=20160907_Newsletter:%20Daily&utm_term=Daily.

[23] Executive Order 13584, *Developing an Integrated Strategic Counterterrorism Communications Initiative* (Sept. 9, 2011); Simon Cottee, *Why It's So Hard to Stop ISIS Propaganda*, THE ATLANTIC (Mar. 2, 2015), http://www.nationaldefensemagazine.org/archive/2016/April/Pages/USProceedingwithNewStrategy toCounterISIL.aspx; Hayes Brown, "Meet The State Department Team Trying To Troll ISIS Into Oblivion," *Think Progress* (Sept. 18, 2014), http://thinkprogress.org/world/2014/09/18/3568366/think-again-turn-away/.

those governments. One of the reviewers noted that "'it's not the U.S. government that's going to break the [Islamic State] brand. It's going to be third parties.'"[24]

Reloading, the Department of State has now created the Global Engagement Center (GEC), which is designed to enable partners in countries with a majority Muslim population to act as messengers, rather than the State Department delivering information directly.[25] The GEC is supposed to be the single entity in charge of coordinating social media engagement to counter terrorist organizations like ISIS. It promises to engage in "rigorous research and modern data analysis" as well as "create, develop and sustain effective positive alternative narratives consistent with U.S. policy objectives."[26] Unfortunately, while these are appropriate objectives, they seem inconsistent with maintaining rapid-fire engagement like that undertaken by motivated individuals supporting ISIS, who appear to receive little guidance from higher headquarters, but have managed to control the narrative.[27]

Favorable facts must reach the targeted populations quickly to make a difference, however: "Falsehood flies, and the Truth comes limping after it."[28] Information programs encumbered by a cautious bureaucratic process will never be timely enough to make much of a difference. Crowdsourcing appears to be superior to government in every aspect of internet engagement.[29] However, it is

---

[24] Greg Miller, *Panel casts doubt on U.S. propaganda efforts against ISIS*, WASH. POST (Dec. 2, 2015), https://www.washingtonpost.com/world/national-security/panel-casts-doubt-on-us-propaganda-efforts-against-isis/2015/12/02/ab7f9a14-9851-11e5-94f0-9eeaff906ef3_story.html?postshare=901449106173651&tid=ss_tw.

[25] E.O. 13721, *Developing an Integrated Global Engagement Center To Support Government-wide Counterterrorism Communications Activities Directed Abroad* (Mar. 14, 2016), http://www.jurist.org/documents/executiveorders/13721.php.

[26] *Id.*

[27] Philip Kapusta, *The Gray Zone*, SPECIAL WARFARE (Oct.-Dec. 2015 (p. 22), http://www.soc.mil/swcs/SWmag/archive/SW2804/October%202015%20Special%20Warfare.pdf.

[28] Attributed to Jonathan Swift (1710).

[29] Ariana Eunjung Cha, *What Yelp can tell you about a hospital that official ratings can't*, WASH. POST (Apr. 5, 2016), https://www.washingtonpost.com/news/to-your-health/wp/2016/04/05/going-to-the-hospital-read-the-yelp-reviews-first/.

not clear that the State Department understands the importance of nongovernmental involvement.

An additional issue with government agencies disseminating information involves the restrictions setforth in the *Smith-Mundt Act,* which prohibits the domestic distribution of public diplomacy information.[30] *Smith-Mundt* has been interpreted broadly inside the government as prohibiting the dissemination of information by means that *might* be seen by Americans.[31] This creates a difficult standard when the material is online and anyone in the world could potentially see those materials. The federal government shouldn't be attempting to influence U.S. audiences, but when this type of guidance is broadly interpreted it ignores the reality of cyberspace. The result renders U.S. information efforts impotent and cedes the field to terrorists who then control the narrative, unopposed.

Even though *Smith-Mundt* was amended in 2013 to address this issue, it remains unclear how the law will be interpreted going forward.[32] There appears to be residual resistance to distributing information by cyber means because of the potential exposure of American citizens.[33] As a fully realized democratic society, the U.S. is especially concerned about maintaining a reputation for truthfulness in the government. That is not true of every U.S. competitor.

---

[30] Matt Armstrong has written extensively on *Smith-Mundt*, for example at *Smith-Mundt Modernization Act of 2012 Introduced in House*, MOUNTAINRUNNER (May 17, 2012), https://mountainrunner.us/2012/05/smith-mundt-modernization-ac/.

[31] It's unclear at this point whether or when practice will change to match the change in the law.

[32] Mick West, *Debunked: 2013 NDAA Thornberry amendment, domestic propaganda, disinformation*, METABUNK.ORG (May 21, 2012), https://www.metabunk.org/debunked-2013-ndaa-thornberry-amendment-domestic-propaganda- disinformation.t592/.

[33] Nafeez Ahmed, *Your Government Wants to Militarize Social Media to Influence Your Beliefs*, MOTHERBOARD (Nov. 14, 2016), http://motherboard.vice.com/read/your-government-wants-to-militarize-social-media-to-influence-your-beliefs.

C. Russia

The Russians are masters of using cyberspace to advance their information agenda. Russia leverages disinformation on an industrial scale, for example, by spreading misleading claims about Sweden's stockpiling of nuclear weapons, stating that nuclear weapons on a Turkish base were at risk, by persistently denying the presence of Russian troops in Ukraine, and most recently, by leading a misinformation campaign during the 2016 U.S. presidential election.[34] In addition, they have been comfortable allowing, even encouraging, private citizens to engage in offensive cyber activities when they coincide with national interests.[35]

Russia's willingness to engage the private sector in this fashion is one reason that it has been able to remain at the forefront of cybersecurity operationally and diplomatically. Other States have been less willing to take this step. In fact, despite Russia's success with this tactic, the U.S. and other Western countries do everything they can to prevent private actors from engaging in offensive cyber activities. This is reminiscent of continental Europe's reaction to England's mastery of the 14th century's super-weapon, the longbow.

England adopted the use of the longbow early in its history. From the beginning, it was clear the longbow's range and penetration power was superior to those of other weapons of its time. Longbows put crossbows to shame, being only a fraction of the cost, with a much greater firing speed and range. It was a perfect, inexpensive

---

[34] Neil MacFarquhar, *A Powerful Russian Weapon: The Spread of False Stories*, N.Y. TIMES (Aug. 28, 2016), http://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html?_r=1; Shane Harris, "Clinton Foundation: Those *Hacked Files' Aren't Ours,* DAILY BEAST (Oct. 4, 2016), http://www.thedailybeast.com/ articles/2016/10/04/clinton-foundation-those-hacked-files-aren-t-ours.html; *U.S. was reportedly more prepared for Russian cyber attacks than disinfomation campaign*, REUTERS (Dec. 20, 2016), https://venturebeat.com/2016/12/20/u-s-was-reportedly-more-prepared-for-russian-cyber-attacks-than-disinformation-campaign/.

[35] *See* Allen & Leeson, *infra* note 33; Levi Maxey, *Cyber Proxies: A Central Tenet of Russia's Hybrid Warfare*, THE CIPHER BRIEF (Feb. 24, 2017), https://www.thecipherbrief.com/article/tech/cyber-proxies-central-tenet-russias-hybrid-warfare-1092.

weapon for peasants, as it was basically a stick of wood. Masses of peasants armed with longbows were so critical to the defense of the realm that Edward I prohibited all manner of sport among the peasantry except archery, and Edward III made weekly archery practice obligatory, banning other forms of competing activities.[36] Henry VIII compelled longbow ownership and also prohibited activities that competed with the mandatory longbow practice.[37] The result of making archery the only lawful recreational activity for decades was a large mass of superbly capable "special forces" available to the king. England's domination in this field was complete.

England basically maintained its monopoly on longbow use for one hundred and fifty years. This wasn't because wood and peasants were in short supply elsewhere, nor because other rulers didn't know how effective the longbow was, but because other kingdoms lacked the political stability to trust such a powerful weapon in the hands of the rabble.[38] England was favored with the political stability that gave it confidence to encourage a talented and armed population. The opportunity to "crowd-source" longbow techniques and skills significantly improved England's military capability. Currently, Russia is employing a similar strategy in the case of hacking skills.

Although it may not be the most stable State in the world, Russia has enough national coherence that it has allowed a number of private citizens to practice with powerful cyber tools. Russia's level of comfort with its political stability and unity has allowed it to leverage the power of private citizens to perfect the use of a powerful weapon. This hasn't given Moscow a monopoly on cyber weaponry, but has provided a different element to its cyber strategy, meriting

---

[36] Douglas W. Allen & Peter T. Leeson, *Institutionally Constrained Technology Adoption: Resolving the Longbow Puzzle*, THE J. OF L. & ECON. (2015) [*hereinafter* "Allen & Leeson"] p. 683, 688, http://www.peterleeson.com/Longbow.pdf.

[37] Allen & Leeson, p. 689.

[38] England's longbow dominance lasted from about 1332-1428. Allen & Leeson, pp. 683-684.

comparison with the English longbow model.[39] Cyber criminals are allowed to hone their hacking skills and their hacking tools, using both for the advancement of outward-directed criminal enterprises. Russia allows this broad access to a powerful means of warfare, resulting in the development of a trained cadre of cyber operators with ever-improving tools. While Russia must accept the inherent risk that this cyber capability could be turned against the regime's interest, it can also avail itself of this force when the nationalist sentiment can be employed to in advance State interests. The Kremlin is in a position to purchase the loyalty of these groups by acquiescing in the commission of cyber crime, creating a shared interest.[40]

In addition to leveraging patriotic feelings and private cyber expertise, Russia actively manipulates social media for its national security purposes, both internally and abroad. For example, people are hired to post negative comments about anti-Russia articles online, and do the opposite for pro-Russia articles, with the intent to overwhelm rational discourse on Western media sites.[41] These Russian professionals have also used Twitter falsely to report an oil spill and an Ebola outbreak in the U.S., perhaps testing a capability to manipulate public opinion and create confusion and mistrust.[42] Even if these false messages reach only a relatively small number of people, social networks have an extraordinary power to convince people and manipulate opinion.[43]

---

[39] Trend Micro increasingly observes hackers' relationships with official authorities and their participation in conflicts. Max Goncharov, *Russian Underground 2.0*, TREND MICRO (2015), http://www.trendmicro.fr/media/wp/russian-underground-2-0-wp-en.pdf.

[40] Mathew J. Schwartz, *Russian Cybercrime Rule No. 1: Don't Hack Russians*, BANK INFO SECURITY (Sept. 14, 2015), http://www.bankinfosecurity.com/blogs/russian-cybercrime-rule-no-1-dont-hack-russians-p-1934.

[41] Daisy Sindelar, *The Kremlin's Troll Army*, THE ATLANTIC (Aug. 12, 2014), http://www.theatlantic.com/international/archive/2014/08/the-kremlins-troll-army/375932/.

[42] Adrian Chin, *The Agency*, N.Y. TIMES MAG. (Jun. 2, 2015), http://www.nytimes.com/2015/06/07/magazine/the-agency.html?_r=0.

[43] *The Social-Network Illusion That Tricks Your Mind*, MIT TECH. REV. (Jun. 30, 2015), https://www.technologyreview.com/s/538866/the-social-network-illusion-

The U.S. might learn from Russia's use of both social media and private actors. The distinction between the way ISIS uses social media and the way Russia does is that ISIS reports its activities, however mortifying they are, and attempts to spin its own situation to look enticing to recruits. Russia uses social media outlets to manipulate public opinion in ways that aren't apparent, and using means that aren't easily attributable to Moscow. There is evidence that U.S. companies manipulate the news to benefit their perceived interests, as well, so it isn't as if this technique is unknown inside the U.S., it just doesn't appear to be used by the government.[44]

Although the U.S. has been reluctant to employ the "cyber longbow" like the Russians have, there are plenty of examples of private citizens performing useful national security work merely as an unplanned collateral result of acts of conscience or activism. People around the globe have joined to oppose ISIS online, both as individuals and as part of groups like Ghost Sec.[45] Some are actively engaging; others are taking good citizen-type actions such as

---

that-tricks-your-mind/; Sean Gallagher, *Air Force research: How to use social media to control people like drones*, ARS TECHNICA (Jul 17, 2014), http://arstechnica.com/information-technology/2014/07/air-force-research-how-to-use-social-media-to-control-people-like-drones/.

[44] Michael Nunez, *Former Facebook Workers: We Routinely Suppressed Conservative News*, GIZMODO (May 9, 2016), http://gizmodo.com/former-facebook-workers-we-routinely-suppressed-conser-1775461006; Reena Flores, *Hillary Clinton Google suggestions accused of favoring candidate*, CBS NEWS (Jun. 11, 2016), http://www.cbsnews.com/news/hillary-clinton-google-suggestions-accused-favoring-candidate-election-2016/. As noted in the article, Google denies manipulating the results.

[45] Shashank Shekhar, *Desi hackers join cyber war on ISIS: 'Hacktivist' group Anonymous says 1,000 Indians are sniffing out jihadi Twitter accounts and websites*, DAILY MAIL INDIA (Nov. 25, 2015), http://www.dailymail.co.uk/indiahome/indianews/article-3334089/Desi-hackers-join-cyber-war-ISIS-Hacktivist-group-Anonymous-says-1-000-Indians-sniffing-jihadi-Twitter-accounts-websites.html; Jack Smith IV, *Anonymous Divided: Inside the Two Warring Hacktivist Cells Fighting ISIS Online*, TECH.MIC (December 04, 2015), http://mic.com/articles/129679/anonymous-vs-isis-how-ghostsec-and-ghost-security-group-are-targeting-terrorists#.tEWnKSnXD.

reporting Twitter accounts that support terrorist activities. Terrorist attacks in Paris motivated many online to strike back at ISIS.[46]

Individual actions aren't limited to opposing terrorist groups. Hackers have lashed out at China in support of pro-democracy protesters in Hong Kong.[47] The hacker group Anonymous released information about drug-related corruption in Mexico, after finding government action there ineffective.[48] Anonymous also decided to support protests in support of democracy in Hong Kong, taking down thirty government sites.[49] Additionally, a group called the Elves works to counter Kremlin trolls who spread propaganda and disinformation about Lithuania.[50] Child pornography has also become

---

[46] Andrew Blake, *#OpISIS and #OpParis: Anonymous hacktivists to retaliate against ISIS after Paris attacks*, WASH. TIMES (Nov. 16, 2015), http://www.washingtontimes.com/news/2015/nov/16/opisis-and-opparis-anonymous-hacktivists-to-retali/; Swati Khandelwal, "#ParisAttacks — Anonymous declares War on ISIS: 'We will Hunt you Down!,'" *Hacker News* (Nov. 16, 2015), http://thehackernews.com/2015/11/parisattacks-anonymous-isis.html; David Goldman & Mark Thompson, "Anonymous blocks jihadist website in retaliation for Charlie Hebdo attack," *CNN* (Jan. 12, 2015) http://money.cnn.com/2015/01/11/technology/security/anonymous-charlie-hebdo/.

[47] Mary-Ann Russon, *Anonymous brings down 30 Chinese government websites to support Hong Kong protesters*, INT'L. BUS. TIMES (Apr. 13, 2015), http://www.ibtimes.co.uk/anonymous-brings-down-30-chinese-government-websites-support-hong-kong-protesters-1496069.

[48] Rodrigo Bijou, *Governments don't understand cyber warfare. We need hackers*, TED (Dec. 2015), https://www.ted.com/talks/rodrigo_bijou_governments_don_t_understand_cyber_warfare_we_need_hackers/transcript?language=en.

[49] Mary-Ann Russon, *Anonymous brings down 30 Chinese government websites to support Hong Kong protesters*, INT'L BUS. TIMES (Apr. 13, 2015), http://www.ibtimes.co.uk/anonymous-brings-down-30-chinese-government-websites-support-hong-kong-protesters-1496069.

[50] Michael Weiss, *The Baltic Elves Taking on Pro-Russian Trolls*, DAILY BEAST (Mar. 20, 2016), http://www.thedailybeast.com/articles/2016/03/20/the-baltic-elves-taking-on-pro-russian-trolls.html. The group has been compared to the resistance fighters in the region during WWII.

a target of citizen hacker groups.[51] These are all indications that some, at least, see hacking as a legitimate form of citizen action.[52]

To emulate the success of the Russians, the U.S. may have to trust the public with the cyber longbow. Private companies have employed hackers to their advantage, even going so far as using such hackers in the fight against U.S. adversaries. There are some indications the U.S. government might permit private citizens with cyber capabilities to use them wisely in certain circumstances.[53] When the FBI was unable to access the iPhone of the terrorists who killed 14 people in San Bernardino, California – and Apple refused to assist – the Bureau reportedly paid hackers to accomplish the task.[54] The government has also shown signs it will work with hackers to advance national defense, with programs like "Hack the Pentagon," in which it offers a bounty to hackers who find and report vulnerabilities in DoD computer networks.[55]

---

[51] *Anonymous Hacktivist Group Now Gunning for Powerful Pedophile Networks*, SPUTNIK NEWS (Jan 26, 2016), http://sputniknews.com/europe/20150124/1017301478.html#ixzz48LNRiLjF.

[52] Lorenzo Franceschi-Bicchierai, *A Notorious Hacker Is Trying to Start a 'Hack Back' Political Movement*, MOTHERBOARD (May 23, 2016), http://motherboard.vice.com/read/notorious-hacker-phineas-fishers-is-trying-to-start-a-hack-back-political-movement.

[53] Katie Moussouris, *Hackers Can Be Helpers*, N.Y. TIMES (Mar. 30, 2016), http://www.nytimes.com/roomfordebate/2016/03/30/should-hackers-help-the-fbi/hackers-can-be-helpers; Nichole Hong, *U.S. Revamps Line of Attack in Social-Media Fight Against Islamic State*, WALL ST. J. (Aug. 28, 2016), http://www.wsj.com/articles/u-s-revamps-line-of-attack-in-social-media-fight-against-islamic-state-1472415600?utm_source=Sailthru&utm_medium=email&utm_campaign=Defense%20EBB%2008-29-16&utm_term=Editorial%20-%20Early%20Bird%20Brief.

[54] Shane Harris, *Did the FBI Just Unleash a Hacker Army on Apple*?, DAILY BEAST (Mar. 29, 2016), http://www.thedailybeast.com/articles/2016/03/29/did-the-fbi-just-unleash-a-hacker-army-on-apple.html; Kevin Pousen, *Double Cross*, WIRED (May 2016), https://www.wired.com/2016/05/maksym-igor-popov-fbi/.

[55] Statement by Pentagon Press Secretary Peter Cook on DoD's Hack the Pentagon, CYBERSECURITY INITIATIVE PRESS OPERATIONS (Mar. 2, 2016), http://www.defense.gov/News/News-Releases/News-Release-View/Article/684106/statement-by-pentagon-press-secretary-peter-cook-on-dods-hack-the-pentagon-cybe.

Of course, hackers tend to be independent thinkers and actors who have their own conception of right and wrong. One of the bigger challenges presented by these groups includes using their skills to interrupt lawful discourse. For example, groups have acted to prevent a candidate from running for public office and hacked a newspaper because it published information that they didn't agree with.[56] While it's certainly true that most private groups come with significant baggage, there simply is no substitute for crowdsourcing.[57] The opportunity to leverage the efforts of millions of people around the globe to invent, solve, and improve is perhaps cyberspace's greatest strength. No government effort can compete with the results of this type of massive collaboration over the long haul, even if it is as unsavory in its methods as hacking ISIS Twitter accounts with pornography.[58] And, surely no government agency would have rick-rolled ISIS, unleashing the devastating Rick Astley on potential ISIS recruits.[59]

The U.S. has tended to shy away from citizen groups like Anonymous because the groups' often offensive behavior, and, because they sometimes act against the U.S. government's perceived interests. Sometimes the obnoxious activities can't be ignored, but most hacker groups seem generally to be in favor of democratic rule and freedom, so there ought to be much common ground with the

---

[56] *Id.; Catalin Cimpanu, Anonymous Warns US Sen. Ted Cruz to Leave Presidential Race, or Else*, SOFTPEDIA (Mar. 21, 2016), http://news.softpedia.com/news/anonymous-warns-us-sen-ted-cruz-to-leave-presidential-race-or-else -502009.shtml; Waqas Amir, *Hacktivists Shut Down Donald Trump Hotel Collections Website*, HACKREAD (May 21, 2016), https://www.hackread.com/donald-trump-hotel-collections-website-down/.

[57] Dai Davis, *Hacktivism: Good or Evil?*, COMPUTER WKLY. (Mar. 2014), http://www.computerweekly.com/opinion/Hacktivism-Good-or-Evil.

[58] Jacob Bogage, *This hacker is fighting ISIS by spamming its Twitter accounts with porn*, WASH. POST (Jun. 14, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/06/14/this-hacker-is-fighting-isis-by-spamming-its-twitter-accounts-with-porn/?utm_campaign=Defense%20EBB%206-15-16&utm_medium=email&utm_source=Sailthru.

[59] James Geddes, *Hacking Group Anonymous Using Rick Astley Video to Rickroll ISIS*, TECH TIMES (Nov. 28, 2015), http://www.techtimes.com/articles/110795/20151128/hacking-group-anonymous-using-rick-astley-video-to-rickroll-isis-video.htm.

U.S. government. The benefits of exploiting the commonality could be enough to outweigh the negative. The general resistance to cooperating with the government creates an obvious barrier to working with hacker groups, and the challenges shouldn't be underestimated, but the potential is so great the government ought to make an effort. The U.S. should search for those areas of overlapping interests, subtly encouraging, or at least not discouraging, private action in these areas.

Russia appears to have found a way to keep the groups that it works with under control, and the U.S. must do likewise if it intends to make better use of this resource. Russia enjoys the benefit of working with groups motivated by money. Wealth is a straightforward way to secure the cooperation of these groups. Less concrete goals of groups like Anonymous – increased freedom? more free speech? – present a greater, but not insurmountable, challenge.

IV. A WAY FORWARD

One thing that might be preventing more creative U.S. national security activities in cyberspace is how the U.S government defines the actual term "cyberspace." Rethinking that definition should be the first step in any U.S. rebalancing efforts.[60]

The U.S. *International Strategy for Cyberspace* uses the terms "digital infrastructure" and "internet" throughout as stand-ins for cyberspace.[61] Similarly, the Department of Defense (DoD) defines cyberspace as, "A global domain within the information environment consisting of the interdependent network of information technology

[60] The word cyberspace is a bit of a historical accident. Novelist William Gibson is credited with coining the term. He wanted a "really hot name" to use in his novels, and recognized the value of cyberspace because it was evocative of much but "meant absolutely nothing." https://www.brainpickings.org/2014/08/26/how-william-gibson-coined-cyberspace/.

[61] *International Strategy for Cyberspace* (May, 2011), https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[62] Both of these terms suggest an approach focused on the physical aspect of cyberspace, largely ignoring the people and thoughts (content) that make cyberspace important.

A more useful approach looks at cyberspace as "the internet plus the ideosphere." Taking the terms separately, the **internet** is the global communication network that allows computers to connect and exchange information, consisting of hardware such as servers, routers, cables, and switches, as well as the software necessary for the hardware to operate.

The **ideosphere**, on the other hand, is the "place" where ideas are created and grow. It's where thoughts and theories are made and evaluated.[63] As ideas interact, often instantly on a global scale only possible through cyberspace, they change form. The evolution of ideas is in some ways like the evolution of living organisms, but much faster. Ideas fuse, recombine, and evolve rapidly. The basic element of replication in the ideosphere is the meme, which serves in a role analogous to the gene in physical reproduction.[64] There are many aspects of the ideosphere, but it may be simplest to define it as "the universe of ideas."[65] It is here where U.S. adversaries excel, and, as a result, where the U.S. needs to focus.

If strategic thinking about cyberspace were guided by a framework of cyberspace as the internet plus the ideosphere, strategy would be less likely to focus on infrastructure, and more likely to concentrate on engaging with the content in cyberspace. Jim Lewis, Senior Fellow at the Center for Strategic and International Studies puts it this way, "The problem in the US is we're very militarized, so

---

[62] JP 1-02, DOD DICTIONARY (Feb. 15, 2016), http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

[63] Douglas Hofstadter, METAMAGICAL THEMAS: QUESTING FOR THE ESSENCE OF MIND AND PATTERN, 50 (1987).

[64] Google defines meme as "a humorous image, video, piece of text, etc. that is copied (often with slight variations) and spread rapidly by Internet users."

[65] Hofstadter, at 50-51.

we tend to think about attacking infrastructure. The Russian approach is much more political and about trying to manipulate public opinion."[66] A disadvantage of focusing on infrastructure is that everyone has an interest in keeping the internet functional, and that significantly limits engaging with the infrastructure itself.[67] It's the information and ideas that U.S. adversaries are using to their advantage, and information should be a priority for U.S. national security efforts. At least one U.S. ally has taken steps in this direction. Britain's NSA equivalent, GCHQ, apparently engages with terrorist internet content to discredit and embarrass leadership, in addition to issuing false orders to individual terrorists (or potential ones).[68]

Focusing engagement on content rather than infrastructure has the added benefit of avoiding one of the thornier problems of waging cyber-war – attribution. The U.S., for obvious reasons, seeks to avoid negative effects on infrastructure owned by its political allies. Information, on the other hand, can be weighed by reference only to the information itself. Sophisticated technical operations are required to determine whether engagement is appropriate. If information is helpful to an adversary it can be addressed regardless of the source and without effect on infrastructure.[69]

---

[66] Jack Detsch, *In aftermath of the DNC hack, experts warn of new front in digital warfare*, PASSCODE (Aug. 10, 2016), http://www.csmonitor.com/World/Passcode/2016/0810/In-aftermath-of-the-DNC-hack-experts-warn-of-new-front-in-digital-warfare?cmpid=ema:nws:Daily%2520Newsletter%2520%2808-10-2016%29&utm_source=Sailthru&utm_medium=email&utm_campaign=20160810_Newsletter:%20Daily&utm_term=Daily.

[67] Taking down connected networks quickly decreases the utility of the other networks, as well. Metcalfe's Law states that the value of a network is proportional to the square of the number of users, a concept whose implications for military operations will have to be explored elsewhere.

[68] Forno & Joshi, *America is 'dropping cyberbombs' – but how do they work*?, THE CONVERSATION (May 11, 2016), https://theconversation.com/america-is-dropping-cyberbombs-but-how-do-they-work-58476?mc_cid=a6d6f926a2&mc_eid=3284b6aba6.

[69] Consistent with Constitutional protections, which tend to be applied to everyone regardless of nationality.

V. CHALLENGES

The First Amendment's guarantee of freedom of speech may be the single most important right that defines what it means to be an American.[70] A key component of the exercise of free speech is the ability to communicate freely without government interference. Distinguishing protected speech from impermissible speech will always be an issue in the U.S.[71] A particular complicating factor is that often, speech is permissible under some circumstances but not others. Fiction and satire are examples of vehicles that can protect normally unlawful speech. On the other hand, shouting "fire" when there is none could be a lawful (albeit not very funny) joke, but may be unlawful if that same joke resulted in injury or harm for people trying to escape the building in which the joke was made.

An illustration of how challenging putting all this together can be is Microsoft's policy on dealing with "terrorist content." Microsoft's approach includes definitions of prohibited speech (which includes ". . . endorses a terrorist organization or its acts …") and an exclusion for its search engine, which will still be allowed to return content responsive to searches for terrorist content.[72] For the government to engage aggressively to remove content that is damaging to national security (i.e., terrorist recruiting, lethal knowledge like bomb making skills, or offensive propaganda) it must find a way to determine when unpleasant or undesirable speech crosses the line from constitutionally protected to legally impermissible, based on content or context. Microsoft's approach isn't perfect, but it's an example of a corporate citizen taking up the cyber longbow on its own.

---

[70] "If there is any fixed star in our constitutional constellation, it is that no official, high or petty, can prescribe what shall be orthodox in politics, nationalism, religion, or force citizens to confess by word or act their faith therein" *West Virginia v. Barnette*, 319 U.S. 624, 625 (1943).

[71] Matthew Weybrecht, *Free Speech in an Era of Self-Radicalization*, LAWFARE (Feb. 26, 2016), https://www.lawfareblog.com/free-speech-era-self-radicalization.

[72] *Microsoft's Approach to Terrorist Content Online* (May 20, 2016), https://blogs.microsoft.com/on-the-issues/2016/05/20/microsofts-approach-terrorist-content-online/#sm.0000g8l17to0xdtzrca20pluw755v.

The involvement of private entities in national cyber security is particularly important because they can act in ways the government cannot, and act with information they already have in the course of business or from open sources. Many government activities would require accessing online information, yet proposals that make it easier – or even appear to make it easier – for the government to access private information are instantly condemned.[73] The 2013 revelations of Edward Snowden caused a firestorm of protests against the NSA's surveillance activities, even though the spying programs were lawful under U.S law. The passing of the Cyber Intelligence Sharing and Protection Act (CISPA)[74] in 2013 and Protecting Cyber Networks Act (PCNA)[75] in 2015 also caused public outrage.[76] There simply seems to be a consensus, at least among politically active citizens, that the government should not be allowed to access and monitor large quantities of citizens' data, even to better ensure the security of the U.S.[77]

---

[73] Sorcher, *Digital activists begin broad, grass-roots battle to fight anti-encryption bill*, PASSCODE (Apr. 15, 2016), http://www.csmonitor.com/World/Passcode/2016/0415/Digital-activists-begin-broad-grass-roots-battle-to-fight-antiencryption-bill?cmpid=ema:nws:Daily%2520Newsletter%2520%2804-15-2016%29&utm_source=Sailthru&utm_medium=email&utm_campaign=20160415_Newsletter:%20Daily&utm_term=Daily.

[74] CISPA directs the federal government to conduct cybersecurity activities to provide shared situational awareness enabling integrated operational actions to protect, prevent, mitigate, respond to, and recover from cyber incidents. https://www.congress.gov/bill/113th-congress/house-bill/624.

[75] This amends the National Security Act of 1947 to require the Director of National Intelligence (DNI) to develop and promulgate procedures to promote: (1) the timely sharing of classified and declassified cyber threat indicators in possession of the federal government with private entities, non-federal governmental agencies, or state, tribal, or local governments; and (2) the sharing of imminent or ongoing cybersecurity threats with such entities to prevent or mitigate adverse impacts. https://www.congress.gov/bill/114th-congress/house-bill/1560.

[76] https://static.newamerica.org/attachments/2885-coalition-letter-from-55-civil-society-groups-security-experts-and-academics-opposing-pcna/Coaltion%20Letter%20Strongly%20Opposing%20PCNA.b24d1869025848cb96385603d8208dea.pdf.

[77] Deena Zaru, *Dilemmas of the Internet age: privacy vs. security*, CNN (Mar. 29, 2014), http://www.cnn.com/2015/02/04/politics/deena-zaru-internet-privacy-security-al-franken/.

Even the FBI's request for Apple to crack the encryption on the iPhone belonging to the San Bernardino shooter has generated outrage in a large segment of the population.[78] U.S. citizens have an increasing fear of governmental violations of privacy. A majority of the American people don't trust the government, and are concerned that the government's access to private information will result in violations of privacy and free speech.[79]

From the FBI's perspective, this was an easy call. The phone's owner was dead, along with the privacy interests, and his phone may have contained information to help stop other terrorist attacks. Although Apple didn't have the ability to crack the phone's encryption, it seemed the corporation would be best positioned to develop the capability to assist in the case.[80] The privacy community (and Apple) saw it differently, however.

Apple asserted that developing the technique would set a dangerous precedent and would create a threat to the data security of its customers.[81] In the end, Apple refused to budge and the FBI contracted with an information security company that was able break the encryption on the phone so the FBI could access the information.[82]

---

[78] Kim Zetter, *Apple's FBI Battle Is Complicated. Here's What's Really Going On*, WIRED (Feb. 18, 2016), https://www.wired.com/2016/02/apples-fbi-battle-is-complicated-heres-whats-really-going-on/.

[79] A recent study conducted by Pew Research Center found that only 19% of Americans trust the government. Henry Gass, *How do Americans view government? Survey finds both distrust and hope*, CHRISTIAN SCI. MONITOR (Nov. 23, 2015), http://www.csmonitor.com/USA/Politics/2015/1123/How-do-Americans-view-government-Survey-finds-both-distrust-and-hope.

[80] *See* Zetter, *Apples FBI Battle is Complicated. Here's What's Really Going on*, WIRED (Feb. 18, 2016), https://www.wired.com/2016/02/apples-fbi-battle-is-complicated-heres-whats-really-going-on/.

[81] Tim Cook, *A Message to Our Customers* (Feb. 16, 2016), http://www.apple.com/customer-letter/.

[82] Julia Edwards, *FBI paid more than $1.3 million to break into San Bernardino iPhone*, REUTERS (Apr. 22, 2016), http://www.reuters.com/article/us-apple-encryption-fbi-idUSKCN0XI2IB. After the FBI reported it had accessed the phone, Apple demanded that the FBI tell it about the vulnerability used so the weakness could be patched. Conner Forrest, *Apple demands to know how FBI cracked*

Constitutional protections have given U.S. citizens the freedom to take risks and be creative, and the ability to push back against government programs that implicate privacy or personal property. This arrangement greatly facilitated the success of the U.S. economy and, as a result, U.S. international relations. Of course, the irony in the situation is that the very freedoms that facilitated the U.S. rise to superpower status in the physical world now impair U.S. efforts to be similarly dominant in cyberspace. By contrast, cyberspace has given U.S. rival States and groups another chance to be dominant, and some of them are seizing it with both hands. The lack of freedom may have limited rival States' innovation and progress previously, but the same set of circumstances allow their leadership to push forward in cyberspace, unconstrained by concerns over privacy and other constitutional rights. There must be a middle ground that would permit U.S. activities in the area to advance national security and still provide appropriate protections, even if not absolute dominance, for citizens' privacy.

VI. CONCLUSION

Cyberspace is constantly shifting as new nodes are added and others disappear. Locations of interest move (a network address can change) and are concealed (a network address can be spoofed) with ease. National security laws and strategy were conceived with physical boundaries in mind, but national borders in cyberspace are porous and uncertain.[83] These factors increase the complexity of cyber operations. Defining cyberspace more accurately as two separate elements, infrastructure and content, may help to refocus U.S. strategy going forward.

San Bernardino iPhone, TECH REPUBLIC (Mar. 30, 2016), http://www.techrepublic.com/article/apple-demands-to-know-how-fbi-cracked-san-bernardino-iphone/.When and if the government has an obligation to disclose vulnerabilities is another fascinating debate that is beyond the scope of this article.

[83] Miller, Brickey & Conti, *Why Your Intuition about Cyber Warfare is Probably Wrong*, SMALL WARS JOURNAL (Nov. 29, 2012), http://smallwarsjournal.com/print/13573.

The success of others in the ideosphere, particularly Russia and ISIS, is frustrating, because it is precisely the type of thing Americans are typically good at. Generally, the U.S. does well in the ideosphere (freedom, culture, etc.), but is not as successful as other actors in driving towards specific goals. If the U.S. hopes to operate more successfully in cyberspace it needs to look at things differently. There will be occasions where engaging on cyber infrastructure will be the best tactic, certainly when it is in conjunction with armed conflict. In other cases, maximum effectiveness will be found in taking on the adversary in the ideosphere. Examples may include debating issues, undercutting positive adversary information, manipulating information and the trust placed in it, and preventing the efficient flow of that information.[84]

England's dominance in 14th century military affairs wasn't due to a secret weapon that no one else could obtain. Rather, England's military reigned supreme in the era because its adversaries feared empowering the public to fully participate in national security. The dominance endured until England's rivals decided the rewards of extending capability beyond the elites to the population outweighed the risks. America's adversaries have successfully weaponized social media.[85] How long will it be before the U.S. unleashes its own cyber longbow, employing non-traditional assets for the on-going clashes in cyberspace?

Rather than remaining merely another of the "weary giants of flesh and steel," there is a need for the U.S. to engage in "the new home of Mind."[86] U.S. leadership in cyberspace is vital to ensure it remains a powerful, albeit flawed, force for progress and creation.

---

[84] Maybe sending comedians to engage with ISIS, as the band U-2's Bono suggests, would help solve the problem. Or maybe not. *Bono: send Amy Schumer and Chris Rock to fight Islamic State*, THE GUARDIAN (Apr. 13, 2016), https://www.theguardian.com/music/2016/apr/13/bono-send-amy-schumer-chris-rock-fight-islamic-state-isis.

[85] Emerson T. Brooking & Peter W. Singer, *War Goes Viral*, THE ATLANTIC (Nov. 2016), http://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/.

[86] John Perry Barlowe, *A Declaration of the Independence of Cyberspace*, ELECTRONIC FREEDOM FOUND. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence.

Competing will require employing citizens in the protection of the nation, primarily addressing the information that represents human interaction and all the inherent risks and rewards, with the physical components of the internet playing a supporting role.

Penn State
Journal of Law & International Affairs

2017 VOLUME 5 NO. 1

A RESEARCH AGENDA TO IMPROVE DECISION MAKING IN CYBER SECURITY POLICY

Benjamin Dean and Rose McDermott

TABLE OF CONTENTS

I. SECTION 1

A. Introduction

A lot of recent media attention and an enormous amount of taxpayer dollars have been focused on issues surrounding cyber security. Problems arise because many people mean many different things in referring to cyber security, and different groups have different, often conflicting or even mutually contradictory goals, in pursuing such policy. Some companies and users privilege security; the government places a premium on surveillance, and users vary in their concerns regarding privacy, often not fully understanding the relationship between personal and technical aspects of the term.

Much of the debate around cyber security has generated more heat than light, especially in the wake of the Snowden revelations, often because those who know a lot about the technical aspects of cyber issue know little and care less about government concerns, while those in the policy arena are often willfully unaware of the technical aspects of the domain they are expected to regulate. Everyone can agree that no one wants a foreign country to infiltrate their infrastructure or compromise their financial, transportation, medical, utility or nuclear weapons systems. And everyone agrees that cyber-crime and exploitation are common problems that need to be addressed. But very few know how to go about it.

Many of the discussions around cyber security seem to go around in circles with very little forward progress, in part because the decision-making that generates such policy remains poorly informed and systemically hindered. Here we hope to begin to improve decision-making by providing a theoretical rubric for understanding the underlying factors that influence decision-making across different levels and fields of discipline. In addition, we hope to highlight some of the inherent difficulties in developing successful policy within each step and between areas of inquiry. We then offer a research agenda to guide research into improving decision-making going forward.

1. *Levels of Analysis.*

By the term 'cyber security policy', we refer to policy interventions that coordinate and direct resources toward improving cyber security. Improving cyber security involves protecting computer networks and systems and the users of these technologies (including people and organizations) against physical and financial loss. Decision-making contributes to the formulation of policy interventions at four levels: international, national, organizational, and individual.

Interventions differ across levels. For instance, treaties or agreements are used at the international level, laws and regulation at the national level, and internal policies or codes of conduct at the organizational level.

[Table 1 on following page]

Table 1: A conceptual framework for cyber security policy decision-making

Level	Entities	Factors influencing decision making	Common policy interventions
International	Nation state, international fora and organizations	Lack of institutional structure for non-state actors Diffusion of power No enforcement mechanism Rigidity	Agreements Treaties
National	National government, legislative or executive branch	No national strategy Dispersed responsibility	Law Regulation
Organizational	Private enterprise or governmental administrative agency	Lack of evidence base Rigidity Lack of technical knowledge Lack of coordination and communication between technical experts and policymakers	Company policy Code of conduct Contracts
Individual	Individual person	Loss aversion Uncertainty/information asymmetry	Heuristics Hacker culture Decision making norms

At an international level, the system for mediating relations between nation states is not built in a way that allows for inclusion of non-state actors, which are inherent to any issue connected to digital technologies and the Internet. This, coupled with the dispersion of power among states, individuals and non-state actors, makes enforcement of international treaties or agreements difficult, even if they are agreed upon and enacted.

At a national level, the lack of national strategy and dispersed responsibilities for cyber security policy lead to contradictory policy proposals and unintended consequences that ultimately reduce overall cyber security. There is often a lack of communication and integration between the public and private sector, both of which operate in this space simultaneously. In addition, governments and technology firms may have entirely antagonistic goals in certain areas, including those involving privacy, security and surveillance, as the confrontation between the FBI and Apple over unlocking the San Bernadino shooter's iPhone so richly illustrates.

At an organizational level, deficiencies in the information or evidence base with which to make decisions mean that 'good' programs are not identified and 'bad' ones are not eliminated. This problem is coupled with, and compounded by, a chronic lack of technical knowledge in those organizations with responsibility to respond to cyber security matters, and a simultaneous lack of understanding of policy needs and processes within the technical community.

At an individual level, loss aversion in a situation that is inherently uncertain systematically restricts optimal decision making by encouraging individual leaders to revert to automatic and natural psychological strategies and procedures in decision-making. These strategies and procedures may not be well suited for the complex problems or challenges they confront. Risk can be mitigated through processes, such as insurance, in ways that uncertainty cannot. Uncertainty tends to make people more cautious, especially in the wake of potential catastrophic failure; this puts defenders at a disadvantage relative to attackers.

The decision-making by entities at each of these four levels are influenced by various factors, not all of which work in the same direction. Various incentives and disincentives, constraints and heuristics or biases influence the way in which policy mechanisms are developed, or the ways in which people behave in response to policy interventions. Some of these factors are unique to one level and some apply to many (e.g. lack of information, rigidity, dispersed power).

It is our contention that the development and deployment of policy interventions are influenced by various institutional, organizational, human psychological and behavioral, economic and political biases or heuristics. These influences become encoded in the decision-making mechanisms themselves, which in turn, push those who are subject to the interventions to behave or react in ways that mirror the biases or heuristics or the designers of the interventions themselves.

The cyber security field is in constant flux, and issues related to decision-making are inherently multidisciplinary, which necessitates timely, ongoing and integrated research to keep our societies as productive and secure as possible. In listing the factors that influence decision-making, we draw on the disciplines of international relations, economics, organizational behavior, cognitive and behavioral sciences, psychology and public policy.

How then can we make better decisions in cyber security policy? Section one provides an overview of the obstacles to effective decision-making in cyber security policy at the international, national, organizational and individual levels. A number of interventions might be instituted to try to begin to overcome the various factors that negatively influence decision-making in cyber security policy. In the third section, we propose some specific examples linked to the systemic factors we identify as influencing decision-making in section two. The last section offers a research agenda designed to support the development of the proposed interventions we discuss in section 3.

II. SECTION 2

This section provides an overview of the obstacles to more coherent and coordinated cyber security policy across levels (international, national, organizational and individual) by discussing issues within each level, describing what has been done in the past and in some cases describing the past limitations to success.

A. International

1. *Lack of Institutional Architecture to Deal with Non-State Actors.*

Within international relations theory, the realist school of thought characterizes the international system as anarchic. It is one in which individual states each act in their own self-interest, unable to cooperate out of mistrust of one other. The international system is one comprising Westphalian nation states. This model has prevailed since the treaty for which the system owes its name in 1648. The liberal school of international relations theory called for the creation of a set of international organizations and norms to manage the relations between states in this otherwise anarchic international system.

The Internet, as a network of networks, is not bound strictly by national boundaries in law or in practice, since communication across borders in this system is constant. Cyber-security thus presents a problem that an international system comprised of nation states is ill equipped to solve. So-called 'non-state' actors fill the ecology of cyber-security, from private companies that develop the software and hardware, private Internet service providers, organized criminal outlets and individual 'hackers', not to mention both business and personal users of the Internet. While there is some interaction between state and non-state entities, such as relationships between Russian law enforcement and intelligence agencies with organized criminal groups,[1] and between the Chinese military and semi-autonomous hacking groups, these non-state interests are not present

[1] *See* BRIAN KREBS, SPAM NATION (Sourcebooks, Inc., 2014).

within the delegations representing the respective nation states in international organizations and fora.

A patchwork of international agreements and treaties are linked to cyber-security.[2] One multilateral agreement, drafted under the aegis of the Council of Europe, is The Budapest Convention on Cyber Crime. Signed in 2001, it is open to non-European signatories and has the objective of pursuing, "a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation."[3] The Budapest Convention has attracted 50 signatories. However, it is still criticized as being outdated and has not gained the support of key countries in cyber security such as Brazil and Russia.[4]

On a bilateral level, a number of recent agreements have been created with the intention of curbing cyber-espionage between the United States and China,[5] between China and the United Kingdom,[6] China and Germany[7] and between China and Russia.[8] Questions have been raised as to whether or not the bilateral agreements, particularly

---

[2] *See* Jonathan Clough, *The Budapest Convention on Cybercrime: Is Harmonisation Achievable in a Digital World?*, MONASH U. (July 30, 2013), http://www.aic.gov.au/media_library/conferences/2013-isoc/presentations/clough.pdf.

[3] *See* Council of Europe (COE), CONVENTION ON CYBERCRIME, (Nov. 23, 2001), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561 (last visited Oct. 25, 2016).

[4] Brian Harley, *A Global Convention on Cybercrime?*, COLUM. SCI & TECH. L. REV. (Mar. 23, 2010), http://stlr.org/2010/03/23/a-global-convention-on-cybercrime/.

[5] Colin Lecher, *US Reaches Economic Cybersecurity Agreement with China*, THE VERGE (Sept. 25, 2015), http://www.theverge.com/2015/9/25/9399187/obama-china-cyber-security-agreement.

[6] Danielle Correa, *China and the UK Sign Cyber-Security Agreement*, SC MAG., (Oct. 22, 2015), http://www.scmagazineuk.com/china-and-the-uk-sign-cyber-security-agreement/article/448578/.

[7] Kevin Sawyer, *Germany and China Reach Agreement to End Commercial Cyberwar*, NAT'L MONITOR (Oct. 29, 2015), http://natmonitor.com/2015/10/29/germany-and-china-reach-agreement-to-end-commercial-cyberwar/.

[8] Lee Munson, *Russia and China Sign Cyber Security Pact, Vow Not to Hack Each Other*, NAKED SECURITY (May 11, 2015), https://nakedsecurity.sophos.com/2015/05/11/russia-and-china-sign-cyber-security-pact-vow-not-to-hack-each-other/.

the one between the United States and China, can actually be enforced and thus will achieve their stated goals. Moreover, the agreements leave out other vital organizations such as civil society organizations, critical infrastructure, and the government, military, intelligence, and law enforcement organizations of the respective countries.[9]

Finally, attempts have been made to include 'Internet-based surveillance systems' in the Wassenaar Arrangement, a multilateral agreement on export controls for conventional arms and dual-use goods and technologies. The proposals to extend the Wassenaar Arrangement have been criticized on the basis that, in the long run, it would undermine cyber-security by criminalizing the very security research activities that result in the identification and correction of vulnerabilities in software and hardware.

2. *Diffusion of Power.*

One of the megatrends identified by the National Intelligence Council in its report, *Global Trends 2030: Alternative Worlds*, is the increasing diffusion of power globally.[10] In this increasingly multipolar world, power shifts to networks and coalitions made up of non-state actors such as private enterprises and individual threat actors such as hackers. Ironically, this diffusion and dispersion of power is partly driven by vast improvements in communication technologies. These conditions make it difficult to implement and enforce international agreements even when there is general consensus and agreement on a specific cyber security policy at the international level.

"Who do I call if I want to call Europe", is a quote commonly misattributed to Henry Kissinger in reference to the difficulty in international relations and negotiations when dealing

[9] Richard Bejtlich, *To hack, or not to hack?*, BROOKINGS (Sept. 28, 2015), https://www.brookings.edu/blog/up-front/2015/09/28/to-hack-or-not-to-hack/.

[10] *See Generally Global Trends 2030: Alternative Worlds*, NAT'L INTELLIGENCE COUNS. (Dec. 2012), https://www.dni.gov/index.php/about/organization/global-trends-2030.

with a dispersed entity that has no single representative. The quote nicely encapsulates the current problem facing cyber security policy at an international level between nation states: there is simply no one body or entity to call or to convene major stakeholders to address cyber security threats or challenges.

The international diplomatic system has trouble integrating the views of entities outside of the Westphalian system of nation states. The Internet is a decentralized network of networks that involves privately owned entities in almost all countries. In this aspect, the Internet's greatest strength inherently incorporates its greatest weakness; designed to survive a nuclear conflict, redundancy is baked into its very structure but at the expense of the ability for central administration. As with the nation state system itself, there is no central controlling actor or actors capable of forcing compliance on all participants. International negotiations require the participation of these private entities, yet the international system is not built to incorporate such actors, and so remains unable to include them in ways essential to the success of any treaty in this domain. And yet without the inclusion of such groups and individuals, any international agreement is doomed to failure from the outset.

In fact, this diffusion of nation state power is compounded by the very 'empowerment of the individual' that the Internet itself facilitates. This term refers to the way that digital technologies invert traditional power dynamics. Now individuals, with very few resources, are able to influence the actions and behavior of governmental or multinational organizations many times their own size. Suicide bombers provide a dramatic example of this phenomenon. The influence of individual non-state actors is particularly relevant in cyber security. Many of the threat actors in this field are organized criminal outfits, in many cases backed explicitly or tolerated by the state in which they reside. Widespread availability and adoption of commercially available information communication technologies grants individuals capabilities to access and amplify information previously only available to nation states. And destructive effects are not limited only to organized groups, but can reside within the reach of individual hackers themselves as well.

Effectively controlling such a system through a slow moving and rigid set of decision-making rules, procedures and processes, such as those that characterize the international system, is an immensely difficult task. Even were binding agreements to be reached, actual implementation of these agreements presents a whole new set of difficulties. And enforcement proves harder still, especially in the fast-moving technological landscape. These is a deep and persistent, perhaps unfathomable breach, between the speed of government and bureaucratic action, and that of technological innovation. In such a contest, technology is bound to circumvent particular restrictions long before those constraints can be implemented. And this is likely to be true for the foreseeable future.

B. National

In organizations there are at least four reasons why planners tend to fail when attempting to address complex problems.[11] First, people tend to oversimplify the process of problem solving to save time and energy.[12] Second, people are overconfident in their own abilities, and thus try to repeat past successes.[13] Third, people have trouble quickly absorbing and retaining the large amounts of information necessary to understand dynamic, ever-changing processes.[14] Finally, people tend to focus on immediately pressing problems at the expense of considering longer term or more distant challenges or the unintended consequences and problems that solutions can create.[15]

These four characteristics of poor decision-making help us understand why the current approach to cyber security policy making at a national and organizational level is failing.

---

[11] *See* DIETRICH DÖRNER, THE LOGIC OF FAILURE: RECOGNIZING AND AVOIDING ERROR IN COMPLEX SITUATIONS (Basic Books 1989).

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *Id.*

1. *No National Strategy*.

In the United States, there is no national strategy and no long-term strategy for cyber security policy. This creates a vacuum of responsibility and an absence of direction and constraint which leads to contradictory policy. This inevitably generates the emergence of turf wars over the rapidly expanding Federal funds available for programs nominally meant for 'cyber' purposes, but often directed toward other only tangentially related interventions by agencies which seek to co-opt these funds for other purposes.

This is not a new problem, nor one restricted solely to the domain of 'cyber' for that matter. In 2013, the Government Accountability Office released a report entitled, '*National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*'.[16] Specific problems identified with the cyber security policy approach include: few milestones or performance measures in government strategy documents; the assignment of high-level roles and responsibilities but important operational details being left unclear; and wide variance across cyber security strategy documents in terms of priorities and structure, how they link to or supersede other documents, and how they fit into an overarching national cyber security strategy.[17] Little has changed to improve these deficits in the intervening years.

The Department of Defense's Cyber Strategy, perhaps the longest standing national strategy document, provides a set of strategic goals but lacks fine-grained, operational details that are publicly available.[18] The Comprehensive National Cybersecurity Initiative was released in 2013 and came with 12 initiatives but did not come with an operational plan on how these initiatives should be

---

[16] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-187, CYBERSECURITY: NATIONAL STRATEGY, ROLES, AND RESPONSIBILITIES NEED TO BE BETTER DEFINED AND MORE EFFECTIVELY IMPLEMENTED (2013).

[17] *Id.*

[18] *The DOD Cyber Strategy*, THE DEP'T OF DEFENSE (Apr. 2015), http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

implemented and operationalized.[19] The Cybersecurity National Action Plan came with a set of actions, like setting up a Commission on Enhancing National Cybersecurity, and creating a Federal Chief Information Security Officer position, and allocated $19 billion in funds across a plethora of activities, but did not include tangible outcomes and metrics for determining cost effectiveness or 'success'. This is a combination tailor-made for inciting misuse of government funds.

The responsibilities for portions of cyber security policy are spread out across dozens of Federal agencies, the Department of Defense and intelligence community, regulators and other ancillary bodies (like Information Sharing and Analysis Centers, or ISACs). This dispersed responsibility, coupled with no overarching strategy, creates situations where agencies pursue cyber security policy goals that match their organization's interests but, in many cases, contradict the cyber security concerns of other organizations, sectors, and people, or produce unnecessary, wasteful, or even deleterious redundancies, often even without awareness of such duplication. Lack of fully transparent communication between these divisions within the government serves to further complicate problems associated with disaggregated policy planning and implementation.

A recent example is the push by FBI Director Comey for laws that would mandate backdoors to be placed in encryption standards. Were this policy to be successfully implemented, it would have the effect of weakening overall cyber security (including the cyber security of other government agencies), not to mention the ability of foreign actors to access sensitive American materials.

Another example is the National Security Agency, which has a dual mission that in practice is contradictory. The Signals Intelligence mission requires that the agency acquire the communications of foreign governments (espionage). The second mission of the NSA, the Information Assurance mission, tasks the agency with safeguarding the information of government agencies,

---

[19] *The Comprehensive National Cybersecurity Initiative*, EXECUTIVE OFF. OF THE PRESIDENT OF THE U.S., https://www.whitehouse.gov/sites/default/files/cybersecurity.pdf (last visited Sept. 25, 2016).

corporations and individuals in the U.S. The approach is summarized as 'keep our information safe, get theirs.'

The Signals Intelligence mission requires that key information technology infrastructure, hardware and software, be weakened and exploited. These technologies, in many cases are the same ones used by government agencies, corporations and individuals in the United States itself. The weakening of these technologies puts these entities in the U.S. at risk (the revelation in 2016 of back-doored Juniper routers, which are used by many U.S. Federal government departments, is a case in point). Add to this the fact that US Cyber Command, which is the military's designated organization for safeguarding its networks and information, is led by the same person that leads the NSA, and we have a muddled set of responsibilities with little coordination.

C. Organizational

1. *Lack of Evidence Base.*

Evidence-based policy making is an approach where policy decisions are based on the collection and interpretation of objective evidence relating to the policy issue at hand and the performance of the policy option implemented. Its intellectual roots lie in evidence-based medicine, where randomized controlled trials are used to assess the policies or treatments that contribute most toward the resolution of a particular condition or ailment. This etiology embodies an important corrective; fixing one problem in the human body often causes another because systems are enmeshed in ways that are not always obvious, clear or systematic. Similarly, in a network design like the Internet, focusing on simple, easy-to-measure outcomes can quickly become a version of the drunkard's search. Just as lowering cholesterol does little to change overall risk of coronary artery disease, although the ability to do so with statins makes billions for Big Pharma every year, reducing the number of hacks may not necessarily mean the overall system is safer. After all, body counts in Vietnam did little to provide an accurate indicator of how well the United States was doing in that war. Effective decision-making in

complex environments requires knowledge about the structure of a system and the outcomes of the decisions made in relation to the goals that are being pursued.[20] Without this knowledge, an organization may implement interventions that ultimately exacerbate the very problems that it seeks to mitigate.

In cyber security policy, there is a dearth of reliable, verifiable data on the financial scale of the losses, the sources of threats and risks, and the potential positive and negative impacts of policy decisions. While figures on the number of cyber incidents are released annually by the Computer Emergency Response Team (US-CERT), such figures are methodologically questionable – for instance - much of the increasing incidence figures could be chalked up to better detection methods and companies have incentives to hide serious breaches - and thus give very little in the way of policy-relevant guidance.

Where there are metrics available, there is no guarantee that they will be actionable, relevant or useful. For instance, since 2003 the Department of Homeland Security has been operating an intrusion detection system, formerly called the National Cybersecurity Protection System, now called the EINSTEIN program.[2122] After over a decade of operation, and $6 billion in investment, "none [of the metrics developed by DHS] provide insight into the value derived from the functions of the system."[23] An estimated $19 billion was allocated to cyber security measures in the 2017 White House budget proposal, representing a 35% increase

---

[20] *See* DÖRNER, *supra* note 11.

[21] It is of great concern therefore that the Cybersecurity National Action Plan calls for the Department of Homeland Security to enhance Federal cybersecurity, "by expanding the EINSTEIN and Continuous Diagnostics and Mitigation programs".

[22] Aliya Sternstein, *US Homeland Security's $6B Firewall Has More Than a Few Frightening Blind Spots*, DEFENSE ONE (Jan. 29 2016), http://www.defenseone.com/technology/2016/01/us-homeland-securitys-6b-firewall-has-more-few-frightening-blind-spots/125528/.

[23] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-16-294, INFORMATION SECURITY: NHS NEEDS TO ENHANCE CAPABILITIES, IMPROVE PLANNING, AND SUPPORT GREATER ADOPTION OF ITS NATIONAL CYBERSECURITY PROTECTION SYSTEM (2016).

over the previous year.[24] However, it was not clear where all these funds were going because there was no definition for what actually constitutes a 'cyber security program'.[25] Even data on research and development (R&D) spending on cyber security, the release of which is required by law, have only been made available as recently as 2013.[26]

The lack of reliable evidence is due to a number of reasons. There are strong incentives for corporations and government agencies not to disclose whether an information security failure has occurred, facilitated in part by patchy data breach notification laws, which are set at a state level in the United States, and differ substantially in their requirements. Companies may not want competitors to know their weaknesses, and corporations as well as the government may not want the public to lose faith that their personal financial, medical, or social information is safe when they interact with them. This of course assumes that the company is aware of a failure in information security having even taken place, which is far from guaranteed.

Where there are data and studies available, the most commonly cited data sources are compiled by security or antivirus vendors, who have business incentives to magnify the problem, or are in studies undertaken by academic institutions or think tanks and sponsored by corporations that operate in the field. These studies make unrealistic assumptions about the behavioral responses of companies, and do not take into account the unobserved differences among companies in the datasets. They assume that all companies react in the same way to information security incidents regardless of industry, size (whether by headcount or annual revenues), business model or current revenues, costs or profitability. In reality, the losses

---

[24] *The President's Budget for Fiscal Year 2017*, THE WHITE HOUSE: OFF. OF MGMT. AND BUDGET, https://www.whitehouse.gov/omb/budget (last visited Sept. 26, 2016).

[25] *Middle Class Economics: Cybersecurity*, THE WHITE HOUSE: THE PRESIDENT'S BUDGET, FISCAL YEAR 2016 (Aug. 7, 2015), https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/fact_sheets/cybersecurity-updated.pdf.

[26] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 16.

that a company might face from a security breach are influenced by the individual company's fragility, which in turn is a function of a number of firm-level characteristics including customer loyalty, profit margins or debt. For a hypothetical example, if a company with low profit margins, low customer loyalty and high debt is subject to a costly data breach, and that information becomes public, the periodic drop in revenues and curtailed access to short-term debt might render the company insolvent. This would not be the case for a company with high margins, high customer loyalty and low debt. Yet many studies treat all companies as if they were identical when predicting or forecasting potential impacts of a breach.

Selection bias is also endemic. The only companies that appear in malware or data breach incident datasets are those that: a) detected the incident; b) subsequently reported the incident; and c) were able to accurately quantify the impact of the incident. Of the entire universe of companies, only a fraction of a fraction is likely to be included in this analysis. Simple methodological problems like ensuring a representative sample are endemic in commonly used, self-reported surveys. The total losses across countries are often based on extrapolations for entire populations; multiplying the average loss per company by the total companies in the country or economy may not provide the most accurate estimate of actual breaches or losses.[27]

This lack of evidence means that cyber security policy makers cannot determine where the true problems lies and where policy interventions might have the greatest benefit given their costs, nor can they track the subsequent outcomes of the policy interventions that they make. This failure then compounds over years as successful policy interventions aren't identifiable and failed policy interventions are allowed to persist in spite of their failure.

With no basis on which to evaluate the need for and effectiveness of cyber security policy, there is a risk that the system becomes nothing more than a 'self-licking ice cream cone': A self-

[27] Dinei Florencio & Cormac Herley, *Sex, Lies and Cyber-crime Surveys* (Microsoft Research, Working Paper), *available at* https://www.microsoft.com/en-us/research/wp-content/uploads/2011/06/SexLiesandCybercrimeSurveys.pdf.

perpetuating process that is meant to address a problem but instead contributes to the very problem that it is ostensibly designed to solve.

2. *Chronic Lack of Technical Knowledge.*

The chronic lack of technical knowledge and talent within the organizations with responsibility for cyber security policy severely hampers these organizations' ability to effectively develop and implement policies. This technical knowledge gap can be attributed to there being no standard way in which to classify or keep track of cyber security related roles, and to the inability of Federal agencies to retain and develop what technical talent they are able to hire.

Again, this problem is not new. In 2011, the Government Accountability Office released a report titled '*Cybersecurity Human Capital: Initiatives need Better Planning and Coordination'*, flagging that, "eight agencies with the biggest IT [information technology] budgets have trouble handling their cybersecurity workforces and determining their composition and responsibilities."[28] It remains a persistent problem. In a 2013 report, the GAO wrote that, "only 2 of 8 agencies it reviewed developed cyber workforce plans and only 3 of the 8 agencies had a department-wide training program for their cybersecurity workforce."[29] The Department of Defense was the only agency to report their shortage to the GAO in 2011 (as they were the only ones who had a methodology in place).

This has not stopped government agencies from announcing large hiring targets, complete with large budgets, to hire cyber security personnel. The Department of Defense announced that it would have 6,000 'cyber-warriors' by 2016 but there is little indication of where these people would come from (much less what a 'cyber-

[28] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-8, CYBERSECURITY HUMAN CAPITAL: INITIATIVES NEED BETTER PLANNING AND COORDINATION (2011).

[29] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 16.

warrior' does). The Office of Personnel Management was also competing to hire 1,000 cyber security personnel in this market.[30]

The Department of Homeland Security is the private sector's liaison on cyber security matters – it also advises other agencies on the issue. The GAO identified 1,361 cyber security personnel at DHS in their 2013 study. One official is quoted as saying, "the National Cyber Security Division has had trouble finding personnel for certain specialized areas, such as watch officers".[31] This division has a central role in operating important interventions such as the EINSTEIN system, developing the National Cyber Incident Response Plan, and operating the National Cybersecurity Center.

The lack of any data to measure the problem or outcomes of policies to address the problem makes achieving strategic goals, like Initiative #8 of the *Comprehensive National Cybersecurity Initiative*, which calls to, "develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees," even more challenging.

Another underlying reason for the chronic lack of technically skilled people in government is that government can rarely compete with the private sector in the IT arena in terms of salary, stock options, prestige and other remunerations. Few career public servants have an advanced understanding of technical issues in the area of cyber security, and even fewer private sector IT professionals have any understanding of, much less interest in, the processes underlying the formulation of government policy. At a cultural or ideological level, many of those who work in or are a part of the tech industry either in Silicon Valley or more generally have a Libertarian or Randian bent. They are broadly skeptical of and distrust government,[32] exacerbating the conflict between government and industry in the surveillance versus privacy debate around cyber security goals. Even if the government could compete head-to-head

---

[30] GOVERNMENT PUBLISHING OFF., https://www.gpo.gov/fdsys/pkg/FR-2015-11-10/html/2015-28566.htm (last visited Sept. 26, 2016).

[31] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 16.

[32] A compact summary of this set of values can be found in Richard Barbrook and Andy Cameron's 1995 essay 'The Californian Ideology'.

in pay, it would still have to overcome the ideological forces that dissuade Silicon Valley from collaborating openly with government.

The security and screening requirements for many positions related to cyber security in the Federal government have created obstacles to hiring talent as well. One example is Ashkan Soltani, who was in line to work with the White House's Office of Science and Technology Policy after a stint as the Federal Trade Commission's Chief Technologist, but whose security clearance application was rejected possibly due to past affiliation with Edward Snowden.[33] In another example from 2014, the Director of the Federal Bureau of Investigation stated that the agency was considering relaxing its policy, which prohibited hiring anyone who had used cannabis in the past three years, because it was so difficult to find candidates for cyber security roles who would pass the policy's requirements.[34]

Simultaneously, private entities with the skill base to address some of these challenges technologically have no ostensible reason to include policy experts on their design teams. Government does not mandate or regulate such participants, and there is little or no support or infrastructure in most technology companies for their contribution. On the other side of the equation, it is hard enough for the government agencies to find people to manage and secure their internal information technology networks, let alone find those with the technical knowledge and skills coupled with an understanding of public policy formulation and implementation. Both sides are thus confronted with enormous challenges to achieving mutual understanding and translation of basic needs and goals.

Finally, government organizations typically set their cyber security policy internally as a list of compliance-based check boxes that the system administrators are expected to rigidly follow. These

---

[33] Danny Yadron, *White House denies clearance to tech researcher with links to Snowden*, THE GUARDIAN (Jan. 29, 2016), https://www.theguardian.com/technology/2016/jan/29/white-house-tech-researcher-denied-security-clearance-edward-snowden-nsa.

[34] Leo Kelion, *FBI 'could hire hackers on cannabis' to fight cybercrime*, BBC NEWS (May 22, 2014), http://www.bbc.com/news/technology-27499595.

check box lists are developed from the perspective of the defender, not the adversary, so they are typically circumvented by highly resourced and sentient adversaries. Their 'one size fits all' approach emphasizes attaining compliance over actually directing resources towards areas where dynamic risks are greatest for the organization in question.

The management of government agencies also does not permit the system administrators who manage their IT networks the autonomy necessary to take a proactive approach to system security. These rigid policies are the equivalent of handcuffing the security guard at the front of the building and then telling him/her to keep the place safe from thieves. A long-term effect is that, rather than empowering the system administrators to proactively address cyber security concerns, this approach drives out the most talented technical employees, thereby compounding the already acute skills shortage in Federal agencies.

D. Individual

1. *Heuristics and Biases.*

Clearly many challenges confront our ability to formulate effective cyber-security policy. Not least among these are systematic and predictable barriers which exist in the minds of individual decision makers and other stake-holders. A few of these merit some comment, specifically roadblocks related to loss aversion and the difficulties of making decisions under conditions of uncertainty. These proclivities can induce a kind of paralysis because people find themselves averse not only to change, but especially to risks and threats that incorporate some element of uncertainty.

Loss aversion constitutes a well-known phenomenon first experimentally documented in the work of Daniel Kahneman and Amos Tversky.[35] This work elegantly demonstrated human hedonic

[35] *See* Daniel Kahneman & Amos Tversky, *Prospect Theory: An Analysis Of Decision Under Risk*, 47 ECONOMETRICA: J. OF THE ECONOMETRIC SOC'Y 263, 261-

asymmetry. In short, people are more averse to loss than they are attracted to an equal gain. So, for example, it hurts more to lose $10 than it makes most people happy to win $10. In fact, people need to be offered about $25 on average to make them indifferent between a bet which can lead to a loss of $10. In other words, most people need two and a half times more potential benefit in order to take the risk of a potential loss. This phenomenon in and of itself can, of course, lead to a particular kind of paralysis since it embodies an inherent status quo bias. People will of course seek out uncomplicated gains, but if a path also poses a risk, people will, on average, show a relatively high degree of loss aversion.

There is, however, one important consistent exception, as described in Prospect Theory.[36] When people are operating in a so-called domain of losses, when things are bad and look to be getting worse, people become much more prone to taking risks, including quite dramatic ones, in order to recoup previous losses, and return to the former status quo position.

There are a couple of important caveats in this work. Most relevant, people will show the opposite tendency, meaning risk aversion in the domain of losses, when probabilities are low. This explains, for example, the almost universal acceptance of insurance whereby people pay a sure cost to avoid the very small probability of a larger loss. But note there that these assessments of likelihood typically result from subjective assessments and not necessarily objective probability, meaning that people can often misjudge how likely a given event may be. This would certainly be especially likely in a domain such as cyber-security where the base rate of risk is largely unknown as we noted above. While it makes sense that any given company or entity may want to keep successful attacks secret, this lack of transparency makes it much more difficult for the overall community to accurately assess the objective threat and share important information on successful defensive strategies. This secrecy works to the attackers' advantage. Greater dissemination of accurate information about kinds and types of attack, even within

---

91 (1979); *see also* Daniel Kahneman & Amos Tversky, *Choices, Values, and Frames*, 39 AM. PSYCHOLOGIST 341, 341-50 (1984).

[36] *Id.*

closed networks, might allow for the development of more effective counter-strategies, or even more effective insurance policies to amortize risk across the broader system, even if such allocation were restricted to specific sectors or industries.

In policy terms, this translates into some potentially destructive consequences. In short, people are more likely to take risks that could make things worse precisely when they are already in bad circumstances. This can easily snowball to make things a lot worse very quickly. These are the times when caution might be most warranted, but is also less likely, particularly in an environment permeated by a sense of crisis, time pressure or high stakes. Thus, policy makers may prove loath to develop policies to implement if disaster strikes when things are going well, for fear of offending potential allies and donors, because of distraction from more pressing problems at any given moment, or due to general status quo malaise. However, once a crisis hits, pressure mounts, and that sense of threat and risk is precisely what throws decision makers into a domain of loss where the potential for optimal decision making is restricted, and in the absence of well-developed and rehearsed standard operating procedures, catastrophic losses become much more likely to occur simply as a result of momentum. Under such conditions of attack, risk acceptance dominates, especially because the crisis itself shifts leaders' perceptions regarding the probability of subsequent attack.

This entire process may characterize decision-making in any number of domains but becomes exacerbated by the uncertainty that typically permeates cyber-attacks in particular. Decision making under uncertainty often proves difficult. In general, such decisions, particularly when time is of the essence, are dominated by a series of so-called judgmental heuristics[37] which provide useful rules of thumb for filling in the blanks when objective probabilities remain unknown. Their exact operation remains outside the purview of this discussion and can be found elsewhere.[38] For our purposes, suffice it to say that

[37] Amos Tversky & Daniel Kahneman, *Judgment under Uncertainty: Heuristics and Biases*, 185 SCI. 1124, 1124-31 (1974).

[38] *See* ROSE MCDERMOTT, RISK TAKING IN INTERNATIONAL POLITICS: PROSPECT THEORY IN AMERICAN FOREIGN POLICY (University of Michigan Press, 1998) (discussing an application to political science).

uncertainty, like risk, can systematically restrict optimal decision making by encouraging individual leaders to revert to established psychological strategies and procedures in decision making that may not be well suited for the given problems or challenges they confront. Recall that such biases evolved precisely because in most circumstances they offer fast and easy and largely accurate responses to the world; in other words, they developed precisely because, on average, they allow largely accurate estimates in the absence of objective information at the lowest cognitive cost. However, it is precisely in novel or unusual circumstances, such as those often posed by cyber-security challenges, where we might expect the systematic operation of such biases to induce predictable biases leading to sub-optimal results.

However, this need not necessarily be the case. Sometimes, embracing the wisdom of uncertainty can precipitate unexpected creativity in decision-making. Admittedly, this is most likely when the decision-making milieu is not riven by time pressures, which is why systematic planning prior to crisis becomes essential to avoid the more negative consequences of psychological bias in decision making. Conversely, when planning can take place at a time of relative security, the acceptance of uncertainty can help generate unexpected solutions and opportunities because individuals come to see that the standard operating procedures do not properly address new challenges which exist in domains divergent from those areas which the original procedures were designed to address. For example, standard operating procedures designed to respond to a military assault on a physical location will not offer much guidance when the attack occurs in virtual space, however real the financial, logistical or operational consequences of cyber breaches. Therefore, it is precisely the inherent uncertainty of the new environment that offers the possibility for new and creative responses, but these are only likely to emerge under conditions of calm, not under circumstances defined by threat and the risk, where loss aversion will dominate, and risky choices become more likely.

Thus, it becomes easy to see how the same pattern of unproductive and unresponsive decision-making recurs. When the problem is not salient, it is easier not to do anything, but under

conditions of threat, risky choices predominate, which may not necessarily help future outcomes. As Einstein said, the definition of insanity is doing the same thing over and over and expecting a different result. However, if we change the approach, and embrace the creative possibilities present under conditions of uncertainty in times of calm, it may then become possible to harness human psychological tendencies in our own favor to develop more creative solutions to novel problems.

III. SECTION 3

A. Developing Governance Models that Manage to Diffuse Power and Non-State Actors

The international system has to adapt to a world that is vastly different from that which it was built to manage. Effective cyber security policy development and implementation at an international level will require bringing nation states together with private companies, the technical community, non-governmental organizations, and individual hackers. Faced with diffused power across many linked entities, decision-making structures and processes themselves have to be more adaptable, flexible, bottom-up, and resilient. As with many contemporary global challenges, there is a need for governance mechanisms unlike those that were used to govern the more kinetic international challenges, which dominated international relations prior-to and during the 20th century.

A number of international organizations are attempting to take responsibility for various aspects of cyber security policy at the international level. For example, in 2014, the United Nation's International Telecommunications Union (ITU) called for, "Strengthening the role of ITU in building confidence and security in the use of information and communication technologies."[39] The

[39] International Telecommunications Union [ITU] (2014), Resolution 140 rev Busan 2014: Strengthening the role of ITU in building confidence and security in the use of information and communication technologies,

ITU membership brings together governments and the private sector (including Sector Members, Associates and Academia) to forge agreements on radio communications standards and increasing development through greater access to information and communication technologies (ICTs).

The problem for organizations such as the United Nations and other international fora is that they either do not or can only partially include the diverse state and non-state stakeholders that comprise the cyber security field. In addition, their typical programs of work have timelines that span many years. In the time it takes to complete one cycle, a field like cyber security usually moved on to new and more pressing issues.

One model worth examining more closely is the Internet Engineering Task Force (IETF), which has done a good job over the past two decades providing a forum in which technical experts and organizations can come together to make decisions relating to the technical architecture on which the Internet operates. This process has been effective because of its open format – anyone can join the meetings – its rough consensus system for reaching agreement, and the Request for Proposal system, which ensures that all participants have an opportunity to make proposals and then debate these proposals. These characteristics have resulted in technically robust and agreed upon technical standards and outcomes for the Internet.

B. National – A National Cyber Security Plan

Following Dörner's original findings, addressing complex problems requires the establishment of an overall plan with clear goals, a 'systems level' understanding of the environment in which the plan will be executed, and iterative revision of the plan in response to information updates on the state of play. Components of a coherent plan to guide cyber security policy at a national level include a long-term strategy with clear goals, milestones, performance targets, resources, and responsibilities.

---

https://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res. 130.pdf (last visited March 7, 2016).

For the first time, as a follow-up to the 30-day 'cyber sprint',[40] an operational plan was released on October 30, 2015 to upgrade Federal cyber security in the United States. The White House *Cybersecurity Strategy and Implementation Plan (CSIP)* was intended, "to identify and address critical cyber security gaps and emerging priorities, and make specific recommendations to address those gaps and priorities."[41] It had 5 overarching objectives:

- Prioritized identification and protection of high value information and assets;
- Timely detection of and rapid response to cyber incidents;
- Rapid recovery from incidents when they occur and accelerated adoption of lessons learned from the Sprint assessment;
- Recruitment and retention of the most highly-qualified cyber security workforce talent the Federal Government can bring to bear; and
- Efficient and effective acquisition and deployment of existing and emerging technology.

[40] After realizing that over 14 million personnel records had been stolen from the U.S. government Office of Personnel Management, a 30 day 'cybersecurity sprint' was announced. The goal was to take, "number of steps to further protect Federal information and assets and improve the resilience of Federal networks". In tangible terms, some steps included the patching of critical vulnerabilities, acceleration of the implementation of multi-factor authentication, and tightening of policies and practices for privileged users. Progress reports were required after 30 days (The White House, 2015c). What's extraordinary is that, after tens of billions of dollars in prior investment, these basic steps had not yet been implemented.

[41] Memorandum from The Executive Office of the President to Heads of Executive Departments and Agencies (Oct. 30, 2015), *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf.

Each of these 5 objectives was given a set of concrete goals linked to the achievement of the objectives. Its timeline clearly laid out the steps that had to be taken, and allocated responsibility to the respective organizations in order to achieve the stated objectives before September 2016.

This plan was a major first step in a very narrow part of the U.S. Federal Government's efforts to implement basic cyber-security measures among selected Federal departments. This approach should be replicated to cover cyber-security policy nationally for the public and private sectors.

As a part of the development of this plan, a clearer and less contradictory allocation of authority and responsibilities for key portions of cyber security policy is required. The announcement of a Chief Information Security Officer, who focuses on coordinating cyber security across federal agencies, and is housed within the Office of Management and Budget at the White House, is a promising first step in this direction.[42]

However, the announcement of the possibility that the Signals Intelligence and Information Assurance responsibilities within NSA may be merged, two functions that are in practice contradictory, was a possible step in the wrong direction.[43] A far better alternative would have been to allocate the Signals Intelligence mission to the NSA, the government and military Information Assurance mission to US Cyber Command (which would have to be led by a different person than the head of the NSA), and the private sector Information Assurance mission allocated to where it resides at present with the Department of Homeland Security (with the Chief Information Security Officer potentially playing an oversight or coordination role). Such an arrangement would have avoided the

---

[42] Danny Yadron, *White House seeks its first ever chief information officer*, THE GUARDIAN (Feb. 9, 2016), https://www.theguardian.com/technology/2016/feb/09/white-house-seeks-first-chief-information-security-officer-hackers-cybersecurity-hacking.

[43] Danny Yadron, *NSA merging anti-hacker team that fixes security holes with one that uses them*, THE GUARDIAN (Feb. 3, 2016), https://www.theguardian.com/technology/2016/feb/03/nsa-hacker-cybersecurity-intelligence.

prior conflict of interest by separating the offensive capabilities, by housing them in the Department of Defense, from the defensive capabilities, by housing them in the Department of Homeland Security.

C. Organizational

1. *Improving the Evidence Base.*

More robust evidence would contribute greatly to better cyber security policy and filling the chronic lack of technical knowledge that has emerged in Federal agencies. Creating a mechanism where private companies are required to report breaches while ensuring the secrecy of such information might go far toward creating a more comprehensive data base, while assuring such firms that their leaks would not risk unnecessary public distrust or the exposure of proprietary code or information.

There needs to be standard definitions for what cyber security budget spending actually constitutes and agreed measures for the results or outcomes of these budget items. This is necessary so that money nominally allocated to 'cyber security' is not used for other purposes merely because its meaning can be easily morphed; the result of a policy produced through such aggregation would be hap-hazard at best, lacking integration and overall strategy. This is akin to asking for the input and output measures for cyber security policies. With these measures in hand, the outcomes of cyber security policy interventions can be evaluated.

Of all fields, development economics might have tools for potential use in testing cyber security policy interventions. For instance, the logical framework approach (log-frames) has been used for decades to design interventions in many complex fields (e.g. agriculture, education, health) by identifying goals, tying actions to

those goals, and then evaluating the intervention according to pre-established metrics.[44]

Borrowing from the medical field, development economics and development aid organizations have some well-developed tools and principles for the monitoring and evaluation of interventions in complex systems.[45] Participants are randomly allocated to one of two groups, only one of these groups is given the intervention, and then the differences between the groups post-intervention are measured so as to determine its effectiveness or efficiency. However, as with the human body, the Internet is a large network, meaning that changes in one place may affect other parts of the system in unintended or unanticipated ways, and attention to such feedback loops remains an important part of not making things worse by providing a series of bandages that do nothing to stop the bleeding (or to prevent later problems such as infections).

Lessons from this field could be drawn and deployed to give cyber security policy makers a toolkit with which to classify their budget items in a consistent way (the inputs). This then allows measures of the effects of these policies across metrics like the number of breaches per year, or the proportion of designated high-value information that is encrypted, or any measure that is deemed appropriate (the outputs) to be developed, and used to adjust, eliminate or add various program elements to improve performance.

2. *Specialized Track for Technical Talent*.

To improve the level of technical talent in cyber security roles within government agencies, a specialized track for this talent –

---

[44] *See* D. McLean, *The Logical Framework In Research Planning And Evaluation* 1-11 (ISNAR, Working Paper No. 12, 1988); *see also Guidance on using the revised Logical Framework*, DEPARTMENT FOR INT'L DEV. (Jan. 2011), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/253889/using-revised-logical-framework-external.pdf.

[45] *See* Esther Duflo & Michael Kremer, *Use of Randomization in the Evaluation of Development Effectiveness*, http://economics.mit.edu/files/2785 (last visited Sept. 27, 2016); *see also* Abhijit V. Banerjee & Esther Duflo, *The Experimental Approach to Development Economics*, 1 ANN. REV. ECON. 151, 151-78 (2009).

subject to different working conditions and hiring requirements than typical positions – is one avenue worth exploring. Indeed, as part of the Cybersecurity National Action Plan (CNAP), a $62 million educational fund was created, "for Americans who wish to obtain cybersecurity education and serve their country in the civilian Federal government."[46] This was an extension of the already-established National Science Foundation's and Department of Homeland Security's CyberCorps Scholarship for Service program and a sort of Reserve Officer Training Corps program for new cyber security talent.[47] Such a program provides long term benefits to recipients as well as government agencies as a larger pool of experts is recruited and cultivated.

Other existing initiatives might provide lessons for this or other special training initiatives. One might be the US Digital Services (USDS), which was originally modeled on the United Kingdom's Government Digital Service. The USDS is housed within The White House Office of Management and Budget that brings technical, policy and legal professionals and places them in Federal agencies where technical talent is lacking. They take a human centered design approach to the use of technology to make government departments more responsive and accessible to people. They have projects running in areas that have been deemed priorities by the Obama administration including Veteran's Affairs, Department of Homeland Security (linked to immigration, not cyber security), Social Security and the IRS. Their annual budget is partially covered by Congress and partly comes from the partner agencies where their members work.

Another model that might be worth emulating is the Jefferson Science Fellowship Program. This program has existed since 2003 and allows tenured, or similarly ranked, academic scientists, engineers and physicians from U.S. institutions of higher learning to spend one year in Washington D.C. at the U.S.

---

[46] *The President's Budget for Fiscal Year 2017*, *supra* note 24.

[47] *See* Sean Gallagher, *Obama wants you to join CyberCorps Reserve to help feds get their act together*, ARS TECHNICA (Feb. 9, 2016), http://arstechnica.com/tech-policy/2016/02/obama-wants-you-join-the-cybercorps-reserve-to-help-feds-get-their-act-together/.

Department of State or the U.S. Agency for International Development (USAID). A similar program might be developed for cyber security talent, in U.S. higher education establishments or even private sector companies (given that some of the best talent resides in the financial sector), to do a yearlong service in government agencies where their technical talent or specialized knowledge could be used to improve the organization's cyber security or strategy in this area. Such a program might also potentiate important and on-going social networks between government and technical experts, and allow each to achieve a greater understanding of the other's needs, incentives, goals and constraints.

Each of these programs may not be able to compete financially with the private section, but by harnessing existing talent, supporting emerging talent, and trying to attach service and prestige to government work, such strategies can help to improve the current reservoir of skill within existing agencies.

D. Individual

Of course, the structural incentives identified can be shifted through organizational changes to induce greater compliance and attention to issues surrounding cyber security, including enhanced transparency and improved integration and communication across agencies tasked with different but overlapping goals. But ultimately the causal agents within any organization are individuals who remain subject to the inherent psychological biases we discussed above.

1. *Transparently Structured Choices and Consequences.*

It is not easy, but there are some standard ways to reduce individual's susceptibility to such biases.[48] First among these is simply to make people aware of the unconscious biases that may affect their judgment and decision-making. The simplest way to do this is not through complicated, time-consuming, expensive training programs during which people zone out. Rather, the idea is to make sure that

[48] *See supra* note 35, at *Id.*

choices are structured in a transparent way so that such biases become evident. For example, in the classic experiment where people had to make real life choices between radiation and surgery for cancer, options were presented with "mortality" and "survival" statistics side by side. When this is done, the equivalency of the options becomes immediately evident, but the psychological pull across framing also remains obvious. In a similar manner, choices between options in response to a particular threat should present both the costs and benefits of options side by side, not only for the relevant choices, as is often typically done, but also relative to the status quo (i.e. doing nothing) option so that costs and consequences of inaction become as immediately salient as those associated with any given course of action.

Because people are preternaturally preoccupied with loss, it is important to find ways to convey not only probabilities, but also help people to better understand how to psychologically calibrate the meaning of abstract probabilities. The human mind does not do well with very large numbers; we are all aware of the phenomenon of "crisis fatigue" whereby one dead boy on a beach is a tragedy but hundreds of thousands of refugees pouring into Europe from Syria is an immigration challenge that provokes border controls and political hostility.

These numeracy challenges can play out in myriad ways. One of the best ways to help decision makers contemplate very large data breaches is to encourage strategies or procedures for transforming such issues into very direct and small scale terms. Human psychology is much better suited for solving smaller scale problems; it is much easier for people to get a handle on and contemplate how to respond in a constructive way to challenges that are framed in local terms. So, for example, we can worry about threats to the electrical grid but the initial policy problem that needs to be solved and addressed might be better facilitated if it was framed in terms of how to get electricity back up in Washington, D.C. without cyber capacity, and then scale up from these more local decisions to national policy plans.

2. *Training through Gaming and other Table-Top Simulations for Emotion Regulation.*

Importantly, as much as the Western canon has taught professionals to privilege rationality over emotion, rationality as posited by economists in particular is little more than an intellectual construct completely devoid of psychological reality. Psychological rationality is deeply emotional by design; the human mind privileges emotional information since that is what has been key to survival in the face of myriad threats over millennial time. This means that people are exquisitely sensitive to emotional inputs, perhaps overly so in modern contexts, but as with loss aversion, we are more attentive to negative emotions such as fear and anger than more positive ones such as hope and joy.

Negative emotions, while important and useful for helping us to properly allocate energy and attention, and also to consolidate memory, can nonetheless encourage over-reactions to threats and attacks, especially uncertain ones that pose an ambiguous or uncertain risk. Encouraging training for emotion regulation would be time and money well spent to reduce the risk of over-reaction to uncertain or threatening stimuli. Enormous amounts of evidence now exist documenting the benefits of mindfulness based stress reduction strategies in achieving such goals.[49]

Moreover, this is a domain in which gaming and other table-top simulations positing different kinds of threats and crises could prove helpful in giving people an engaging, even fun, way to gain practice, experience and knowledge about potential response options to any given scenario. Such strategies also work to build a sense of community and camaraderie among those who would have to work together in a real crisis. In this way, issues of dominance, specialization of labor and other issues which can interfere with effective, time-sensitive responses, can be negotiated prior to the actual crisis, so that when real challenges emerge, team coordination and cooperation can be as smooth as might reasonably be expected.

---

[49] *See* P.R. Goldin & J.J. Gross, *Effects of mindfulness-based stress reduction (MBSR) on emotion regulation in social anxiety disorder*, 10 EMOTION 83, 83-91 (2010).

IV. SECTION 4

Research will be required to translate many of the proposals made in the section above into the cyber security policy field. This section outlines a research agenda that is intended to provide some guidance on the kinds of research questions that might profitably be pursued and the research methods that might help yield useful answers.

A. Developing Governance Models that Manage to Diffuse Power and Non-State Actors

An examination of governance models that have either been designed to coordinate diffuse entities, or that have proven to be successful in coordinating diffuse entities, would be a useful step forward in determining a global governance model for cyber security policy. This paper has already mentioned the IETF as a model that has proven successful in the past for managing technical matters related to the Internet globally.

Perhaps there are lessons to be drawn from global governance models in other areas of public health policy, such as the World Health Organization and the Centers for Disease Control, or in conflict mitigation and resource sharing, such as the Arctic Council, or in the establishment of international law, such as the United Nations Conventions on the Law of the Sea?

A comparative examination of these varied arrangements would look at the types of parties involved, the mechanisms by which decisions are made and consensus is achieved, the cost of setting up and maintaining the mechanism (and by whom this cost is borne), the success of the mechanism in achieving its stated objectives, and the reasons for failure should failure be experienced.

One of the challenges with devising a new set of governance strategies with the flexibility and adaptivity that would allow both state and non-state actors, including businesses, to engage is that the Internet itself, as a network of networks, and the World Wide Web, run contrary to most established forms of government structure,

which are hierarchical in nature. While originally hailed as a mechanism to survive and enhance resilience in the case of nuclear war, and later as a means by to encourage and facilitate greater democratic involvement, the Internet also provides a platform where individuals with very few resources can exert almost unprecedented damage and destruction. This structure challenges those who wish to provide an interface between hierarchical and horizontal governance structures to offer a different kind of structure.

One kind of structure that might potentially be considered involves the notion of panarchy as developed by Buzz Holling and colleagues[50] in their work on environmental sustainability. This work developed out of examining how systems in nature achieve balance across large systems over time. In this concept, three factors of capacity, connectedness and resilience emerge most prominent.

The Internet itself offers almost limitless potential for connectedness and great potential for resilience, but this framework raises stark concern about the relative capacity of predator and prey. However, this is where another biological model might prove useful and instructive. Well-established equations such as the Lotka-Volterra[51] which characterizes the predator-prey dynamic would allow similar mathematical modeling of the dynamic interaction between hackers, governments and the businesses who try to survive and thrive in cyber space. Although originally developed in a biological context to represent the impact of disease and competition among animals as a function of numbers, time and rates of interaction to measure prospects for survival or extinction, it has long been used in

---

[50] C.S. Holling, *Understanding the complexity of economic, ecological, and social systems*, 4 Ecosystems 390, 390-405 (2001); Brian Walker et al., *Resilience, adaptability and transformability in social-ecological systems*, 9 Ecology and Soc'y (2004).

[51] A.J. Lotka, *Contribution to the Theory of Periodic Reaction*, 14 J. OF PHYSICAL CHEMISTRY 271, 271-74 (1910); A.J. Lotka, *Analytical Note on Certain Rhythmic Relations in Organic Systems*, 6 PROCEEDINGS OF THE NAT'L ACAD. OF SCI. OF THE U.S. 410, 410-15 (1920); A.J. LOTKA, ELEMENTS OF PHYSICAL BIOLOGY, 71-274 (Williams and Wilkins, 1925); VITO VOLTERRA, VARIATIONS AND FLUCTUATIONS OF THE NUMBER OF INDIVIDUALS IN ANIMAL SPECIES LIVING TOGETHER (R.N. Chapman ed., 1931).

economics to model interaction of sectors in industries as well,[52] and could readily be adapted for use in the context of cyber competition. It has more recently been used successfully to characterize the maintenance of cultures of honor in environments with aggressive actors and weak institutions, a condition not unlike the current state of Internet governance.

This model offers important insight because although it makes a number of important simplifying assumptions, it also highlights how the evolution of predator and prey influence each other. In an evolutionary context, predators select for characteristics that will enhance their ability to find and capture prey, just as prey select for traits that increase their ability to hide, escape or otherwise evade predation. These selection features influence the oscillation dynamics of each side in the equation, precipitating cycles of dominance, but because the goals of predator and prey are antagonistic, the selection of mutually antipathetic characteristics profoundly affects the dynamics of their interaction as well as prospects for survival. These biological models, which exist in well-developed differential equations, and have already been used to positive effect in economics, offer concrete ways to examine the interaction between hackers and defenders, regardless of which sides governments or businesses may be on.

B. A National Cyber Security Plan

The first step in developing a national cyber security plan requires examining what has been done in other countries in the past, as well as seeking to develop innovative solutions for our own particular needs and goals. To date, there is limited comparative literature on the national cyber security plans deployed in countries such as Singapore's 5 year National Cyber Security Masterplan, the United Kingdom's National Cyber Security Strategy, and Canada's Cyber Security Strategy, among many others.

---

[52] R.M. Goodwin, *A Growth Cycle*, *in* SOCIALISM, CAPITALISM AND ECONOMIC GROWTH (C.H. Feinstein ed., 1967).

Comparing the success of other country's plans - which have clear goals, action plans, metrics for success, timelines and responsible agencies - would allow for a comprehensive plan to be written in the United States that learns from the successes and failures of others (rather than repeating any recognized mistakes).

C. Specialized Track for Technical Talent

The first step in considering new policy proposals should be a pre-feasibility study based on cost-benefit analysis. A cost-benefit analysis would look at the financial cost, both to the host organization that would pay for the awardee's stipend, and to the organization from which the awardee is seconded. It then becomes possible to compare this dollar amount to the benefits that would accrue to the host organization and to the alternative policy option of training or hiring talent from scratch. If the costs outweigh the benefits by a certain ratio, then this policy option may not be worth pursuing.

The point of comparing this specialized track to training or hiring from scratch is important. The major strength of creating a specialized track for bringing technical talent into government for the short-term, vis-à-vis the current approach, which is epitomized by proposals to hire 6,000 'cyber warriors' into DoD or 1,000 new personnel into OPM, is that it is will not run into the practical resource constraints that are going to face these other proposals (namely: that there simply aren't enough qualified people in work force to hire at this level for the medium-term). Indeed, a cost-benefit analysis will likely find that the cost effectiveness of a specialized track is many times less than the alternative, which would have the added benefit of freeing up funds to be used for other initiatives with the goal of bolstering cyber security.

D. Improving the Evidence Base

Compiling transparent, reliable, and statistically rigorous cyber security statistics would contribute to better decisions in cyber security policy. The problem to date has been that this responsibility

has been taken on either by organizations with a stake in stoking greater fears about cyber security (e.g. anti-virus companies and private security vendors) or with organizations that lack the requisite statistical capacity to provide reliable data (e.g. the FBI's Internet Crime Complaint Center).

This is typical practice in the U.S., where statistics are compiled by organizations responsible for the regulation of the sector or administration of the sector (e.g. the Federal Aviation Authority compiles aviation data, similarly the National Center for Health Statistics operates under the Centers for Disease Control). Assigning a disinterested party with sufficient statistical capacity and credibility to provide an independent assessment of the scale of the problem could prove very helpful for beginning to design programs to help address these issues. Could the National Institute for Standards and Technology play a role, either as a convener or as an authority to grant some authority to cyber security data?

When randomized control trials were applied from medicine to the development economics field in the late 1990s, there was a need to develop a specialized methodology to respond to the unique logistical and ethical issues that arise in international development work. Adjustments to randomized control trial methodologies will likewise have to be made to adapt them to the unique characteristics of cyber security.

For instance, it isn't clear how comparable control and treatment groups might be identified or separated when so many network elements differ across organizations (indeed, even within organization the elements are likely to differ). The rate at which the technology changes and software is patched might also make it difficult to keep the two groups separate and, within the groups, maintain consistency across subjects (then again, many organizations run on legacy systems that are 10 years old, so this might not be such a great obstacle depending on the organization). This might imply that the studies might only be able to be conducted at the organization-level, though we simply don't know yet.

An assessment of the costs of running an experiment would be useful. The costs of randomized control trials in cyber security

may not be cost-effective. The up-front costs to actually run the experiments may not be overwhelming, especially considering the multi-billion dollar budgets being allocated at a national level, but the cost associated with the losses to the control group may accrue over time and offset the potential gains from the experiment (then again, given that attackers only need to infiltrate one out of potentially thousands of users to compromise a system, perhaps the risk levels remain the same whether undertaking an experiment or not, although the cost may not).

A taxonomy of cyber security 'inputs' and 'outputs' would also have to be developed in order to undertake an experiment. Accurate measures for the effects of treatment would also need to be developed and established. The goal would be to determine which metrics exist and can be reliably measured, or which ones might have to be created, in order to measure effectively the various policy interventions that could be made to reduce certain cyber security risks.

E. Developing Gaming and Other Table-Top Simulations

There is a long and established body of work on gaming and table-top simulations for crisis situations, even in cyber security. Indeed, a recommendation during a panel on mitigating cyber security threats at a recent conference at Columbia University was that, "simulations, war/business games, and table-top exercises can provide additional venues for information sharing and help build trust between participants, which can be helpful in crisis situations."[53]

Indeed, this is where using the intrinsic strengths of the industry itself may be able to potentiate innovative methods for training and testing; the use of simulations can prove enormously helpful by providing a way to control for many elements while

[53] *Proceedings of the Conference on Internet Governance and Cyber Security*, COLUMBIA SCH. OF INT'L AND PUB. AFF. (May 14, 2015), https://sipa.columbia.edu/system/files/Proceedings_ColumbiaSIPA_InternetGoverance_Cybersecurity_Conference2015.pdf.

varying one, and being able to do so across many diverse elements quickly, either simultaneously or sequentially. Once problematic areas are identified using this strategy, more elaborate real time experiments can be conducted manipulating potentially problematic aspects. Any such simulations could be easily conducted using existing Internet based platforms which allow for multi-user simultaneous interaction.

Where new research might be especially useful is in the development of methods that combine psychological training and emotion regulation training with simulations. The idea would be to run through the several stages that comprise risk-based approaches to cyber security, such as the NIST Risk Management Framework, so as to identify where the failure to successfully implement the framework occurs due to panic or individual biases and heuristics, and then address these sources of failure.

V. CONCLUSION

We have described the factors that we believe influence decision making in the area of cyber security across four main levels of analysis: international; national; organizational; and individual. Each poses unique challenges to the development of a coherent and consistent policy of cyber security.

After describing what has been done to enhance cyber security at each level, and noting the challenges that remain, we have suggested some important ways in which policy and research might advance policy in more productive ways. These include: establishing a coherent national plan with clear and coherent benchmarks and policies and plans for implementation and accountability; the conscious development of different governance structures for regulating the Internet internationally; creating a national service action plan for recruiting and circulating cyber talent in and out of government; providing a more accurate evidence base of past experience to improve future response; and establishing regular games and simulations to train people in how to respond to differing potential threats.

Enhancing cyber security is a critically important project. It also appears an overwhelming one on which we have made less progress than those who seek to exploit the systems in question. In developing systems designed more for overall resiliency than security, the architects of the Internet never imagined the widespread use it would achieve. However, this resilience has also resulted in vulnerabilities that now need to be addressed. It will require a great deal of coordinated action on the part of many individuals, users, industry and government actors to improve cyber security without compromising privacy unduly. Working diligently and creatively to achieve such a goal will help make everyone safer and more productive.

Penn State
Journal of Law & International Affairs

2017 VOLUME 5 NO. 1

MAINTAINING INDIVIDUAL LIABILITY IN AML AND CYBERSECURITY AT NEW YORK'S FINANCIAL INSTITUTIONS

*Harry Dixon**

Cybersecurity in the financial sector is of paramount importance. Due to significant cyber intrusions affecting some of the world's biggest banks, in September 2016 New York's Department of Financial Services ("NYDFS") proposed regulations requiring banks and insurance companies to establish cybersecurity programs and designate an internal cybersecurity officer. These rules became final in March 2017. Described as a "first-in-the-nation" effort, the regulations will only affect banks and other financial services providers in New York. However, given New York's outsized influence on the financial services industry, it is likely that this will set a precedent for both state and federal regulators. Thus, NYDFS would do well to set a good precedent.

Unfortunately, at least some of the rules need serious improvement. In particular, the proposed regulations require that either the chairperson of the board or a senior officer certify that the firm's cybersecurity program meets the proposal's requirements. Those submitting the certification could be held individually liable if the organization's cybersecurity program is deficient. This liability includes civil and criminal penalties.

However, this contrasts with NYDFS's rule regarding anti-money laundering ("AML") and Office of Foreign Assets Control ("OFAC") transaction monitoring and filtering programs. Under those rules, there are no criminal penalties for individual directors. Because recent developments in financial institutions suggest that AML policy and cybersecurity policy are significantly intertwined and are not easily separable; to track consistency with developments in federal law pertaining to individual liability in corporations; and to maintain consistency and clarity in the law, the NYDFS should, where appropriate, allow its regulators to pursue criminal liability against individuals.

* Associate, Taylor English Duma LLP, Atlanta, Georgia
University of Georgia, Honors Program 2007 - B.B.A. Economics, *cum laude*,(honors); B.A. History, *cum laude* (honors); University of Georgia School of Law, 2013, Juris Doctor (J.D); and, Certified Anti-Money Laundering Specialist (CAMS). The author would like to thank his family and friends for their support, as well as Cam Piasecki for his commentary and revisions.

TABLE OF CONTENTS

I. INTRODUCTION

Everyday hackers attack financial institutions for a variety of motives. Some hackers target financial institutions for money, others, for "the lulz." Still, others hack financial institutions for political motivations because by doing so, they may cause damage to the global economy.

In any of these scenarios the potential for damage is significant. For example, in 2013 a Kiev ATM began randomly dispensing money throughout the day.[1] When a Russian cybersecurity firm began to investigate, they discovered that the ATM was only the tip of the iceberg: malware had severely penetrated the bank's computers, even sending back video feeds of employees conducting routine tasks throughout the day.[2] The criminal group – comprised of Chinese, Russians, and Europeans – were then able to impersonate bank officers, turn on various cash machines, and transfer millions of dollars from banks throughout the world into dummy accounts.[3]

The largest financial institution hack in U.S. history highlights the damages a hack can cause. The United States Attorney's Office for the Southern District of New York charged Gery Shalon, Joshua Samuel Aron, and Ziv Orenstein in a 23-count indictment in November of 2015.[4] In addition to charging the men with securities fraud and money laundering, the indictment alleged that the men had stolen the personal information of more than 100 million customers.[5] As these examples demonstrate, cybersecurity in the financial sector is of paramount importance.

Due to these attacks, along with other significant cyber intrusions affecting some of the world's biggest banks, the New

---

[1] David E. Sanger & Nicole Perlroth, *Bank Hackers Steal Millions via Malware*, N.Y. TIMES (Feb. 14, 2015), *available at* http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html.

[2] *Id.*

[3] *Id.*

[4] U.S. v. Shalon, Aaron, and Orenstein, No. 15-cr-333 (S.D. N.Y. 2015).

[5] *Id.*

York's Department of Financial Services [*hereinafter* "NYDFS"] proposed regulations[6] requiring banks and insurance companies to establish cybersecurity programs and designate an internal cybersecurity officer in September of 2016.[7] These regulations were the result of years of research that probed weaknesses in financial institutions and then asked for feedback from those institutions regarding their efforts to strengthen their cybersecurity regimes. The results established the groundwork for the basic regulations, subject to a public comment period that closed in November of 2016. The rules became effective on March 1st, 2017.

Described as a "first-in-the-nation" effort,[8] the regulations will only affect banks and other financial services providers in New York; nevertheless, *only* is a relative term. Given New York's outsized influence on the financial services industry the rules will set a precedent for cybersecurity within financial institutions, and, both state and federal regulators may use the rules as a framework for their own cybersecurity rules and regulations. Thus, it is important that the NYDFS set a rigorous, clear standard that reflects reality and assesses liability where appropriate.

Unfortunately, the NYDFS has unintentionally created a conflict amongst their rules. The cybersecurity regulations require either the chairperson of the board or a senior officer certify the firm's cybersecurity program meets the proposal's requirements in an annual certification.[9] Those submitting the certification can be held

---

[6] Hereinafter, unless specified otherwise, the terms "regulations" or "the regulations" should be assumed to be referring to the DFS's proposed regulations discussed here.

[7] Sanger & Pelroth, *supra* note 2.

[8] Governor Cuomo, Press Release, *Governor Cuomo Announces Proposal of First-in-the-Nation Cybersecurity Regulation to Protect Consumers and Financial Institutions*, OFFICIAL NEWS FROM THE OFFICE OF THE GOVERNOR (September 13, 2016), *available at* https://www.governor.ny.gov/news/governor-cuomo-announces-proposal-first-nation-cybersecurity-regulation-protect-consumers-and [*hereinafter* "Governor Cuomo Press Release"].

[9] 23 NYCRR 500: Cybersecurity Requirements for Financial Services Companies, N.Y. DEP'T FIN. SERVS., Section 500.00 (Feb. 2017), *available at* http://www.dfs.ny.gov/legal/regulations/adoptions/rf23-nycrr-500_cybersecurity.pdf.

individually liable if the organization's cybersecurity program is deficient.[10] This liability includes civil and criminal penalties.[11] Such a program is often standard in today's corporate culture.

This rule conflicts with NYDFS's rule regarding anti-money laundering [*hereinafter* "AML"] and Office of Foreign Assets Control [*hereinafter* "OFAC"] transaction monitoring and filtering programs. Under the AML and OFAC rules, there are no explicit criminal penalties for individual directors, nor is there an annual certification procedure.[12] As it follows, a situation could arise where a director would not be liable under the AML rule, but would be liable under the cybersecurity rule.

While such a discrepancy in the rules may not seem important, in the context of financial institutions, data breaches and money laundering often go hand-in-hand, as demonstrated by the above example. Indeed, given the broad scope of money laundering laws, money laundering is almost guaranteed to occur in a data breach of a financial institution, even if the theft only amounts to a penny. But that is not the only reason why cybersecurity and AML rules regarding certification should harmonize. Recent developments in U.S. corporate liability law at the federal level may very well influence individual corporate liability at the state level. Thus, the NYDFS should, where appropriate, allow its regulators to pursue criminal liability on both individuals, and the corporation. This will create clarity in the law; reflect the reality of intertwined AML and cybersecurity policies and close a loophole; and will track federal legal developments.

Part II of this article will briefly explain the background of modern individual corporate liability, cybersecurity, and money laundering. In Part III, the proposed rules will be examined and

---

[10] *Id.* at 500.20.

[11] *Id.* at 500.20.

[12] *See generally NYDFS Issues Final Anti-Money Laundering and Sanctions Rule*, DEBEVOISE PLIMPTON (Jul. 6, 2016), http://www.debevoise.com/~/media/files/insights/publications/2016/07/20160706_nydfs_issues_final_anti_money_laundering_and_sanctions_rule.pdf (discussing final changes to AML rule, including removal of compliance rule and threat of criminal penalties).

explained. As we will see, AML and cybersecurity are so intertwined that it does not make sense to have different standards for what is quickly becoming the same group. In Part IV, this author will propose a modification in accordance with New York corporate liability law that reflects the reality of AML and cybersecurity policy. Part V, consists of the author's closing remarks.

II. BACKGROUND

A. Corporate criminal liability for individuals

New York is the birthplace of corporate criminal liability. In *New York Central & Hudson River Railroad v. United States*,[13] the question before the U.S. Supreme Court was whether Congress had acted constitutionally when, via the Elkins Act, legislators imputed criminal liability to a common carrier where any agents and officers of a common carrier granted an illegal rebate.[14] The Court held that Congress could subject a corporation to criminal punishment solely on the basis of an agent's conduct because the Court saw "no valid objection in law, and every reason in public policy, why the corporation which profits by the transaction, and can only act through its agents and officers, shall be held punishable."[15]

Corporate criminal liability law has existed in some capacity in New York since at least 1948.[16] In those days, the state of New York imposed a $5,000 fine for a corporation convicted of a felony that would lead to imprisonment.[17] At the time, case law suggested that

---

[13] New York Central R Co. v. United States, 212 U.S. 481 (1909). For an excellent discussion of this case and modern corporate criminal liability, *see* Andrew Weissmann with David Newman, *Rethinking Criminal Corporate Liability*, 82 INDIANA L. J. 411, 420-421 (2013) (discussing *New York Central*).

[14] *Id.* at 421.

[15] *N.Y. Cent.*, 212 U.S. at 495.

[16] *See Corporate Criminal Liability in New York*, 48 COLUM. L. REV. 794 (1948) ("under the present state of law, a corporation may be liable for almost any crime perpetrated in connection with corporate activities.").

[17] *Id.* at 794.

directors, officers, or employees acting within the scope of their authority could render a corporation criminally liable.[18]

It was around this time that a theory began to form of holding individuals in corporations accountable for crimes. During the Nuremberg trials after World War II, Justice Robert Jackson, Chief Counsel for the United States at Nuremberg, stated during the trial of industrialist Gustav Krupp that, "the great industrialists of Germany were guilty of the crimes charged in this indictment quite as much as its politicians, diplomats, and soldiers."[19] Other cases followed involving industrialists committing war crimes through their corporations.[20] Still, with the exception of acts constituting war crimes,[21] or blatant statutory violations such as securities fraud, for decades prosecuting individuals for crimes committed in connection with their work at a corporation was uncommon.

H. David Kotz, former Inspector General at the Securities and Exchange Commission and current Managing Director of the Berkeley Research Group, has two theories on why this has occurred. First, historically, companies were much more likely to engage in a settlement process with the government, whereas individuals who faced prison time were much more likely to fight any charges. A recalcitrant individual is not preferable to a prosecutor, who unfortunately tends to be overworked and is trying to resolve a case

---

[18] *Id.* at 795 (*citing*, e.g., People v. Lawyers Title Corp., 282 N.Y. 513, 27 N.E. 2d 30 (1940) (illegal practice of law); People v. Woodbury Dermatological Institute, 192 N.Y. 454, 85 N.E. 697 (1908) (illegal practice of medicine); People v. Globe Jewelers Inc. 249 App. Div. 122, 291 N.Y. Supp. 362 (1st Dep't 1936) (treasurer of the corporation sent out a fake form, simulating a court order)) (footnote omitted).

[19] Chatham House, *What Are the Relevant Legal Principles Relating to the Responsibility of Companies and CEOs for Violations of International Criminal Law?* (2012).

[20] *Id.*

[21] *See* Rule 156, Definition of War Crimes, Int'l. Comm. Of Red Cross (defined as "serious violations of the laws and customs applicable in international armed conflict" and "serious violations of the laws and customs applicable in an armed conflict not of an international character,"), https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule156 (last visited Mar. 30, 2017).

as quickly as possible.[22] Secondly, and on a related note, corporations do not face the negligence or intent requirement that individuals face in criminal prosecutions, nor is there a priority for cases that are novel, challenging, and difficult to prove, which shifted enforcement away from individuals and instead towards more obvious corporate conduct with a lower evidentiary threshold.[23]

Yet, because of a flurry of disastrous financial events ranging from Enron's collapse to the financial meltdown of 2008, the enforcement approach utilized by agencies has changed dramatically in the past decade. For years critics argued that the Department of Justice [*hereinafter* "DOJ"] and the Securities and Exchange Commission [*hereinafter* "SEC"] were not doing much to bring civil and criminal cases against parties involved in the 2008 financial crisis.[24] For example, in 2013 Jed Rakoff, U.S. District Court Judge of the Southern District of New York – no stranger to fraud trials prosecuted by the SEC –, complained that the government was not holding individuals responsible for massive frauds, "speak[ing] greatly to weaknesses in our prosecutorial system."[25]

This sentiment set the stage for a memorandum from Deputy Attorney General Sally Yates in September 2015 that outlines a new DOJ policy regarding individual liability in corporate contexts, which came to be known as the "Yates Memo."[26] Since the memo, the DOJ has increasingly imposed criminal and civil liability for individuals conducting corporate misconduct.[27] This policy also requires

---

[22] Berkeley Research Paper, https://risk.thomsonreuters.com/content/dam/openweb/documents/pdf/risk/white-paper/yates-memo-background-and-its-impact-white-paper.pdf (registration required).

[23] *Id.*

[24] *Id.*

[25] *Id.* (*quoting* Nate Raymond, *Judge Criticizes Lack of Prosecution against Wall Street Executives for Fraud*, REUTERS (Nov. 12, 2013), http://www.reuters.com/article/financial-judge-idUSL2N0IX1B620131113.

[26] Individual Accountability for Corporate Wrongdoing, Sally Q. Yates, Department of Justice, Sept. 9, 2015, https://www.justice.gov/dag/file/769036/download.

[27] Roberto J. Gonzalez & Jessica S. Carey, *The Government's Making AML Enforcement Personal*, NAT'L L. J. (Feb. 22, 2016), *available at* https://www.paulweiss.com/media/3359752/gonzalez_carey__nlj_022216.pdf.

companies to provide "all" relevant facts about "all" individuals involved in wrong doing, regardless of "position, status, or seniority," in order for the company to get any kind of cooperation credit.[28]

The election of President Donald J. Trump makes it unclear whether the Yates memo will continue to be enforced. A March 8, 2017 memorandum from United States Attorney General Jeff Sessions says that violent crime will be a priority for the United States Department of Justice.[29] At least one commentator believes that in a time of shrinking budgets, a focus on violent crime means a shift away from white-collar crime.[30] However, as James Connelly of Womble Carlyle in Atlanta has pointed out, federal policies change slowly.[31] Yates herself believes that the priorities laid out in her memorandum represent core values of criminal justice and are thus not ideological.[32] For the purposes of this Article, we will assume that the Yates Memo is indicative of a long-term trend in federal prosecution.

Similarly, the federal government has become aggressive in pursuing individual wrongdoing in the anti-money laundering ("AML") sector. In *Treasury v. Haider*, Civil No. 14-CV-9987 (S.D.N.Y.), the United States Attorney's Office for the Southern District of New York (acting on behalf of FinCEN at the United States Department of Treasury) issued a 146-page complaint against MoneyGram International's former Chief Compliance Officer, Timothy Haider, for the willful failure to implement an effective

---

[28] Yates Memo, https://www.justice.gov/archives/dag/file/769036/download.

[29] Memorandum, *available at* http://apps.washingtonpost.com/g/documents/world/read-the-memo-sent-by-sessions-on-violent-offenders/2367/.

[30] Bethany McLean, *Why White-Collar Crooks May Be Cheering This Sessions Memo*, YAHOO (Mar. 21, 2017), http://finance.yahoo.com/news/why-white-collar-crooks-may-be-cheering-this-jeff-sessions-memo-133115487.html.

[31] James Connelly, *Trump Administration Likely to Maintain Yates Memo Priorities on Corporate Wrongdoing*, WOMBLE CARLYLE (Feb. 14, 2017), http://www.wcsr.com/Insights/Articles/2017/February/Trump-Administration-Likely-to-Maintain-Yates-Memo-Priorities-on-Corporate-Wrongdoing?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original.

[32] *Id.*

AML compliance program or properly file suspicious activity reports, as required under the Bank Secrecy Act.[33] The acts in that case occurred in New York, among other places. Haider allegedly failed to implement disciplinary or termination policies, contravening legal advice provided to Haider.[34] Despite the fact that Haider had knowledge of the fraudulent activity occurring at MoneyGram by its agents and outlets, he continued to allow those agents and outlets to conduct the fraud through MoneyGram's currency transfer system.[35] The complaint also alleges that Haider knew or should have known specific agents posed an unreasonable fraud risk, which MoneyGram's Director of AML Compliance called "egregious and beyond anyone's ability to doubt that the agent and knowledge and involvement."[36] Nevertheless, Haider did not cut ties with any agents or outlets.[37] Finally, while Haider was in charge SAR analysts were unable to access sufficient information to file SARS because Haider kept each department in a separate "silo."[38] Because of this, they failed to have a coherent diligence process, and ignored warning signs regarding authorizing new agents or outlets.[39] Even though the case is still ongoing, the thoroughness of the complaint, the magnitude of the violations, and the District of Minnesota's denial of Mr. Haider's claim that only financial institutions themselves are liable for the failure to maintain an effective AML program, could all be harbingers of the future.[40]

In terms of individual liability, in New York, "[a] person is criminally liable for conduct constituting an offense which he performs or causes to be performed in the name of or in behalf of a corporation to the same extent as if such conduct were performed in his own name or behalf."[41] Although this statute appears to lack a

---

[33] *FinCEN Seeks Civil Money Penalty and Injunction Against Former Chief Compilance Officer of MoneyGram*, FINCEN (Jan. 2, 2015), http://www.sidley.com /en/news/2015-02_banking_and_financial_services_update (citations omitted).

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] *See generally* Gonzalez & Carey, *supra* note 27.

[41] N.Y. PENAL LAW § 20.25 (2016).

mens rea requirement, New York adopts the Model Penal Code's definitions for "purposely," "knowingly," "willfully," "recklessly," and "negligently."[42] When a *mens rea* requirement is not stated in a criminal statute, the intent is nevertheless established if the defendant acted purposely, knowingly, or recklessly.[43] Thus, corporate criminal liability arises when an individual commits an offense purposely, knowingly, or recklessly. It is unclear whether the New York Attorney General ("NYAG") is prioritizing individual corporate liability, as their counterparts in Washington, D.C. are, but given the language of New York's final rules, described *infra*, as well as New York's reputation as the financial center of the United States, the NYAG is likely to follow suit.

The individual liability is strongest in the cybersecurity rules, so our discussion will begin there.

B. Cyber-Attacks

Cyber-attacks – "an attack initiated from a computer against a website, computer system or individual computer . . . that compromises the confidentiality, integrity or availability of the computer or information stored on it"[44] - are not new.[45] Cyber-attacks take many forms, including: gaining or attempting to gain unauthorized access to a computer system; denial of service attacks; installation of viruses; and unauthorized use of a computer for processing or storing data.[46] The first cyber-attack occurred in 1988 when Robert Tapan Morris – a professor who now works at MIT that was convicted for the cyber-attack – introduced the Morris

---

[42] N.Y. PENAL LAW § 15.05 (2016).

[43] *See generally* the Model Penal Code.

[44] VINCE FARHAT, BRIDGET MCCARTHY, & RICHARD RAYSMAN, HOLLAND & KNIGHT, CYBER ATTACKS: PREVENTION AND PROACTIVE RESPONSES (2011), *available at* https://www.hklaw.com/files/Publication/bd9553c5-284f-4175-87d2-849aa07920d3/Presentation/PublicationAttachment/1880b6d6-eae2-4b57-8a97-9f4fb1f58b36/Cyber-attacksPreventionandProactiveResponses.pdf.

[45] NATO, *The history of cyber attacks – a timeline*, *available at* http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm.

[46] Farhat, McCarthy, and Raysman, *supra* note 44.

worm to determine the size of the Internet.[47] The worm replicated itself to multiple computers through weaknesses in the UNIX system, and slowed down those computers to the point that they were unusable.[48]

At first, the most serious cyber-attacks seemed to focus on government and military servers. For example, in the 2000s, countries as diverse as China, Estonia, and the United States reported hacks on various government servers, as well as hacks on private email servers belonging to high-ranking officials.[49] Nevertheless, by 2010 cyber-attacks on private websites had become a frequent occurrence. To illustrate, throughout December of 2009 and January of 2010 a group calling itself the "Iranian Cyber Army" disrupted both Twitter and the Chinese search engine Baidu to redirect users to a site containing a political slogan.[50] In 2013, some South Korean financial institutions reported a cyber infection resembling past cyber efforts by North Korea.[51]

Indeed, as connectivity throughout the world has increased over the last seventeen years, so too has cyber-attacks.[52] In 2007, the U.S. Computer Emergency Readiness Team, an arm of the Department of Homeland Security ("DHS"), reported 12,000 cyber-incidents. Because DHS defines a cyber-incident as a "violation of an explicit or implied security policy," and provides examples such as denials of service, the unauthorized use of a system for processing or storing data, and attempts to gain unauthorized access to systems or their data,[53] we may infer that cyber-incidents and cyber-attacks are functionally similar, if not identical. By 2009, the number of cyber-incidents had doubled from 2007; in 2012, the number had

---

[47] NATO, *supra* note 45.

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] Brian Fung, *How Many Cyberattacks Hit the United States Last Year?*, NEXTGOV (Mar. 8, 2013) http://www.nextgov.com/security/2013/03/how-many-cyberattacks-hit-united-states-last-year/61775/.

[53] Press Release, Department of Homeland and Security, *Report Cyber Incidents*, DEP'T OF HOMELAND SECURITY, *available at* https://www.dhs.gov/how-do-i/report-cyber-incidents (last accessed Nov. 30, 2016).

quadrupled. It is unclear whether this result occurred due to an increase in attacks, or due to an increase in detection. Regardless, the number of attacks underlines the frequency of cyber-attacks.

Cyber-attacks can have many effects depending on what specific entity is attacked, and the level of the breach. For example, energy company BP reports 50,000 attempted cyber-attacks per day.[54] These intrusions can range from something as harmless (albeit annoying) as taking down the website to keep web browsers from learning more about the company, to a highly-damaging intrusion that steals long-term strategy, confidential project-related employee emails, or proprietary information regarding a company's manufacturing process. The National Nuclear Security Administration, an agency tasked with the military application of nuclear science, records 10 *million* hacks a day.[55] Given that the National Nuclear Security Administration handles nuclear security for the United States and assists the military in determining the effectiveness of nuclear weapons,[56] a successful cyber-attack on this organization could be disastrous to international security.

Financial institutions can suffer greatly from a cyber-attack. For example, in June of 2016 the international consulting firm Deloitte published a report outlining 14 business impacts of a cyber-incident.[57]

---

[54] Michael Tomaso, *BP Fights Off Up to 50,000 Cyber-Attacks a Day: CEO*, CNBC.Com (Mar. 6, 2013), *available at* http://www.cnbc.com/id/100529483.

[55] Jason Koebler, *U.S. Nukes Face Up to 10 Million Cyber Attacks Daily*, U.S. NEWS & WORLD REPORT (Mar. 20, 2012), http://www.usnews.com/news/articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily.

[56] *Our Mission*, NAT'L NUCLEAR SECURITY ADMIN, https://nnsa.energy.gov/ourmission.

[57] *See* Deloitte, Press Release (June 15, 2016)(listing customer breach notifications; post-breach customer protection; regulatory compliance; public relations/crisis communications; attorney fees and litigation; cybersecurity improvements; technical investigations; insurance premium increases; increased cost for debt raising; operational disruption or destruction; lost value of customer relationships; lost contract revenue; devaluation of trade name; and loss of intellectual property).

C. Money Laundering

"Simply put, money laundering is the process of making dirty money look clean."[58] That is money laundering in a nutshell, but the simplicity of the statement hides the complexity of the crime. For example, money laundering is not just about cash; the Financial Action Task Force ("FATF") has demonstrated "that money laundering can be achieved through virtually every medium, financial institution or business."[59] Though once considered integral only with drug trafficking, money laundering is a necessary step in virtually any criminal activity yielding profits.[60]

Criminals launder money for three reasons. First, it represents the lifeblood of the organization allowing members to cover expenses, maintain inventories, bribe officials, expand illegal enterprises, and finance their lifestyles.[61] Second, it would be foolish to take money directly from these enterprises for those purposes, as law enforcement can easily trace the funds' origin.[62] Third, these criminal proceeds can be the target of investigation and seizure.[63] Consequently, criminals have a high incentive to conceal the existence of these funds or make illegal proceeds appear legitimate to confound law enforcement and continue the criminal enterprise.[64]

Generally, money laundering can be divided into three stages: (1) placement, (2) layering, and (3) integration. Placement, as the first step, is "the physical disposal of cash or other assets derived from criminal activity."[65] The funds can be placed into the financial system, or they can be placed into casinos, shops, and other businesses.[66]

---

[58] Study Guide for the ACAMS Certification Examination 13, ASSOC. OF CERTIFIED ANTI-MONEY LAUNDERING SPECIALISTS, (5th ed. 2015).

[59] *Id.* at 14.

[60] William R. Schroeder, *Money Laundering: A Global Threat and the International Community's Response*, FBI Law Enforcement Bulletin, 1 (FBI, D.C.), (May 2001).

[61] *Id.* at 1.

[62] *Id.*

[63] *Id.*

[64] *Id.*

[65] Schroeder, *supra* note 60, at 15.

[66] *Id.* at 15.

Layering, the second step, consists of separating illegal proceeds from their source through layers of financial transactions intended to conceal the origin of the proceeds.[67] Layering "involves converting the proceeds of the crime into another form and creating complex layers of financial transactions to disguise the audit trail, source and ownership of funds."[68] The final step of the process is integration. In integration, money is reintroduced into the economy through various methods making it almost impossible for the funds to be traced back to their illicit origin.[69]

Money laundering affects the economy and society in various ways, and while these effects are present in the United States, they tend to be more pronounced in emerging markets.[70] Consequently, emerging markets serve as effective examples when studying the consequences of money laundering. The World Bank has identified five areas where money laundering affects developing countries:

1. Increased crime and corruption;
2. Damaged reputations and international consequences;
3. Weakened financial institutions;
4. Compromised economy and financial sector; and
5. Damaged privatization efforts.[71]

Let's focus on 1, 3, and 4. It should come as no surprise that when a country is viewed as a money-laundering haven, criminals are likely to go there.[72] This in turn generates more crime and

---

[67] *Id.* at 16.

[68] *Id.* at 16.

[69] *Id.* at 18.

[70] John McDowell & Gary Novis, BUREAU OF INT'L NARCOTICS & LAW ENFORCEMENT AFFAIRS, *The Consequences of Money Laundering and Financial Crime*, U.S. Dep't of State 7 (May 2001).

[71] Paul Allen Schott, *Reference Guide to Money Laundering and Combating the Financing of Terrorism,* THE WORLD BANK & INTERNATIONAL MONETARY FUND, Section II at II-1 (2006)[*hereinafter* "The World Bank"].

[72] *Id.* at II-2.

corruption.[73] Finally, it also encourages bribery in functionaries that are critical to the economy, including lawyers.[74]

Financial institutions face unique threats from money laundering because financial transactions can occur instantaneously. Typically, the risks faced by financial institutions due to money laundering can be categorized as reputational, operational, or legal and concentration risks.[75] Reputational risk is defined as the risk that public perception of a bank's business practices and associations, regardless of their accuracy, will cause a decline in the public's confidence in the institution and its integrity.[76] Operational risk is the loss potential from inadequate or failed internal procedures, whether systems-based or human-based.[77] Legal risk is the risk of lawsuits, adverse judgments, unenforceable contracts, fines and penalties generating losses, increased expenses, or even institution closure.[78] Finally, Concentration risk is the loss potential of a company due to credit or loan exposure to borrowers.[79] For example, when a bank lacks knowledge about a customer, the customer's business, or the customer's status with other creditors, the Bank has concentration risk.[80]

---

[73] *Id.* at II-3.

[74] *Id.* at II-3. Whether lawyers should report a client's suspicious transactions has long been the subject of controversy. *See* AM. BAR ASSOC., STANDING COMM. ON ETHICS & PROF'L RESPONSIBILITY, FORMAL OP. 463, CLIENT DUE DILIGENCE, MONEY LAUNDERING, & TERRORIST FINANCING (May 23, 2013) (providing risk-based control measures to assist lawyers in avoiding aiding illegal activities "consistent with the Model Rules."); Joel Schectman, *U.S. Lawyers Are A Money Laundering Blindspot, Some Argue*, WALL ST. J. (May 11, 2015, 5:30 A.M. ET) (discussing the controversy over whether lawyers in the United States should report suspicious transactions as attorneys must do in the European Union); *See generally* Adam K. Weinstein, *Prosecuting Attorneys for Money Laundering*, 51 DUKE L. J. 371, 372, 378-386 (1988) (arguing that "subjecting attorneys to criminal and civil prosecution violates their clients' right to counsel, right to counsel of choice, and right to effective assistance of counsel.").

[75] The World Bank, *supra* note 71, at II-4.

[76] *Id.* at II-5 (citation omitted).

[77] *Id.* at II-5 (citation omitted).

[78] *Id.* at II-5 (citation omitted).

[79] *Id.* at II-5.

[80] *Id.* at II-5.

Many recent cases highlight the dangers financial institutions face in money laundering. HSBC's recent $1.9 billion settlement with the United States government is a salient example of how money laundering affects financial institutions.[81] HSBC "failed to apply legally required money laundering controls to $200 trillion in wire transfers alone, in only a three year period."[82] In fact, the Bank's inadequacies were so great that the DOJ discouraged HSBC from publicizing the incident to avoid further criminal exploitation of HSBC's compliance gaps.[83]

Money launderers commonly use "front companies," which appear legitimate and engage in legitimate business, but are controlled by criminals.[84] Front companies are not concerned with making a profit; they are concerned with preserving and protecting illegitimate funds.[85] Front companies have access to illicit funds that can be used to subsidize the front company's products and services. As a result, this makes it difficult for legitimate enterprises to compete with those front-companies that need-not rely on the company's actual revenue to continue operations.[86] If a criminal organization gets big enough, the organization can control entire sectors of the economy, which in turn leads to economic instability due to a misallocation of resources from "artificial distortions in asset and commodity prices."[87] Front

---

[81] *See* Heather A. Lowe, *Money Laundering & HSBC – How it affects you*, REUTERS (Jan. 10, 2013, 22:01 GMT) (discussed *supra* and *infra*). HSBC avoided an indictment because state and federal authorities concluded that criminal charges would jeopardize the bank and destabilize the financial system. Ben Protess & Jessica Silver-Greenberg, *HSBC to Pay $1.92 Billion to Settle Charges of Money Laundering*, N.Y. TIMES (Dec. 10, 2012 4:10 P.M.)

[82] *Id.*

[83] James Ball & Harry Davies, *HSBC money-laundering procedures "have flaws too bad to be revealed,"* GUARDIAN (Jun. 5, 2015, 10:10 EDT), http://www.theguardian.com/business/2015/jun/05/hsbc-money-laundering-procedures-flaws-too-bad-to-be-revealed (last visited Nov. 18, 2015).

[84] The World Bank, *supra* note 71, at II-6.

[85] *Id.* at II-6.

[86] *Id.* at II-6.

[87] *Id.* at II-6 (*citing* John McDowell & Gary Novis, Economic Perspectives, U.S. State Dep't, May 2001).

companies can also serve as a tax-evasion vehicle, depriving a country of revenue it would have otherwise received.[88]

In the United States, organized crime has used pizza parlors to launder heroin trafficking proceeds.[89] The "Pizza Connection Trial" lasted from September 30th, 1985 and ended on March 2nd, 1987, making it the longest federal criminal trial in the Southern District of New York at the time.[90] 19 defendants in a Mafia group ranging from Brazil, Sicily, New York and the Midwest were charged in participation of a drug ring trafficking heroin and cocaine, laundering tens of millions of dollars through the use of pizza restaurants as fronts.[91] The case – led by then-federal prosecutor Rudolph Giuliani and involving former-prosecutor Louis B. Freeh– cost millions of dollars to complete.[92] These tens of millions of dollars undoubtedly created the distortions mentioned above, and ultimately 17 of the defendants were found guilty.[93]

In the United States, the methods of money laundering have remained stable for the past ten years.[94] They can be classified as one of the following methods:

---

[88] The World Bank, *supra* note 71, at II-6.

[89] John McDowell & Gary Novis, *The Consequences of Money Laundering and Financial Crime*, ECONOMIC PERSPECTIVES (Dep't of State, D.C.) (May 2001), at 7, http://www.ait.org.tw/infousa/zhtw/DOCS/ijee0501.pdf (last accessed Mar. 26th, 2016).

[90] Ralph Blumenthal, *Acquitted in "Pizza Connection Trial," Man Remains in Prison*, N.Y. Times (Jul. 28, 1988), *available at* http://www.nytimes.com/1988/07/28/nyregion/acquitted-in-pizza-connection-trial-man-remains-in-prison.html.

[91] *Id.*

[92] *Id.*

[93] *Id.* To learn more about the Pizza Connection Trial, *see generally* Shana Alexander, THE PIZZA CONNECTION: LAWYERS, MONEY, DRUGS, MAFIA (1988) (discussing the trial); *see also* John Surico, *How Mafia Pizzeria Drug Fronts Inspired One of the Most Complex Criminal Trials Ever*, VICE (Jan. 28, 2016), http://www.vice.com/read/how-mafia-pizzeria-drug-fronts-inspired-one-of-the-most-complex-criminal-trials-ever ("'It was a trial with no end in sight involving a billion puzzle pieces," said [organized crime expert] David Amoruso . . . "all of its participants – defendants, lawyers, prosecutors, jurors, and the judge - had to do their best not to be driven totally insane.").

[94] *See* U.S. DEP'T OF TREASURY, NATIONAL MONEY LAUNDERING RISK ASSESSMENT 3 (2015) ("This assessment finds that the underlying money

1. Use of cash and monetary instruments in amounts under regulatory recordkeeping and reporting thresholds;

2. Opening bank and brokerage accounts using nominees to disguise the identity of the individuals who control the accounts;

3. Creating legal entities without accurate information about the identity of the beneficial owner;

4. Misuse of products and services resulting from deficient compliance with anti-money laundering obligations; and

5. Merchants and financial institutions wittingly facilitating illicit activity.[95]

By reviewing the above methods, one may notice that all five methods relate to financial institutions. These funds derive mainly from fraud and drug trafficking.[96] Fraud covers a wide range of crimes, like healthcare fraud, federal government payments fraud, and identity fraud.[97] Drug trafficking alone generates an estimated $64 billion in cash per year.[98] Furthermore, recent evidence suggests the severance of customer relationships between U.S. banks and Mexican money exchangers, commonly known as "casas de cambio,[99] "has led to increases in the retention and use of drug-related cash, both in the United States and internationally, which has "shifted money laundering activity from Mexico to the United States."[100]

laundering vulnerabilities remain largely the same as those identified in the 2005 United States Money Laundering Threat Assessment.")

[95] *Id.* at 3.

[96] *Id.* at 2.

[97] *Id.* at 2.

[98] *Id.* at 2.

[99] Hannah Stone, *US Targets Bank in Mexican Money Laundering Crackdown*, INSIGHT CRIME, "Exchange houses which are often used by Mexican criminal groups to launder funds." *available at* http://www.insightcrime.org/news-analysis/us-targets-bank-in-mexico-money-laundering-crackdown

[100] *Id.* at 3.

Now, one can also imagine how a criminal, state actor, or non-state actor might try and bypass cyber-security protocols to commit a crime, and then launder the proceeds of the crime. For example, in 2015 a gang of hackers infiltrated more than 100 banks in 30 countries.[101] At the time of the hack, employees were unknowingly opening emails that allowed hackers to insert malware.[102] This malware manipulated the banks' cyber-security protocols and proceeded to and siphon as much as $1 billion directly from the banks over a two-year period.[103] To cover their tracks the hackers layered the proceeds into their own accounts.[104]

A further example can be found in a FINRA report from February 2016 describing an incident where foreign customers considered to be "high-risk" opened four accounts with an online firm and engaged in patterns of fraudulent trading through the firm's Direct Market Access (DMA) platform.[105] These customers hacked other online broker-dealers' accounts, engaging in a short sale schemes that resulted in large profits for the customers' of the firm through their accounts, and losses in the compromised broker-dealer accounts.[106] FINRA punished the online firm for "failing to establish and implement [AML] policies and procedures adequately tailored to the firm's online business in order to detect and cause the reporting of suspicious activity; and . . . failing to establish and implement a reasonably designed customer identification program to adequately verify customer identity."[107]

Curiously, NYDFS has recognized the intersection of AML and cyber-security on prior occasions such as when the agency issued

---

101 Thomas Bock, *The Convergence of Anti-Money Laundering and Bank Security*, K2 Intelligence (Nov. 2015), *available at* https://www.k2intelligence.com/en/insights/thought-leadership/the-convergence-of-anti-money-laundering-and-cyber-security.

102 *Id.*

103 *Id.*

104 *Id.*

105 FINRA, REPORT ON CYBERSECURITY PRACTICES (Feb. 2015), *available at* http://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.

106 *Id.*

107 *Id.*

its BitLicense regulations.[108] These regulations required financial institutions to have designated compliance personnel and AML procedures that are the same as those for institutions handling traditional, fiat currency.[109]

The United States Department of Treasury's Financial Crimes Enforcement Network ("FinCEN") has also started making the connection between cyber-security breaches and money laundering schemes.[110] FinCEN has recently begun to encourage financial institutions to include information on cyber-security events or breaches on Suspicious Activity Reports ("SARs").[111] Specifically, the guidelines provide guidance for SAR reporting in connection with: cyber-enabled crime and cyber events; the inclusion of relevant cyber-related information in SARs; encouraging collaboration between cybersecurity units and AML units within the same firm; and sharing cyber-related information across financial institutions to combat money laundering, terrorism financing, and cyber-attacks.[112] The efficacy of linking a cybersecurity event to a SAR is evidenced by the Federal Bureau of Investigation's use of a SAR to trace $7 million dollars from a Florida bank account to criminals in Russia and Ukraine that had released a "Zeus" botnet virus to make the fraudulent withdrawal.[113]

The convergence of opinion between government recommendations and consultants in the private sector point to a growing consensus that, while AML and cyber-security practices do not and cannot have complete overlap in their functions, they do have significant overlap in their goals and methods. It would seem that two functions within the same organization with significantly overlapping missions would have similar regulatory liability when

---

[108] *See generally* Bock *supra* note 104.

[109] *Id.*

[110] Chris Kentours, *Cybersecurity and AML: How the Twain Must Meet?*, FINOPS REPORT (Nov. 10, 2016), *available at* http://finops.co/slider/cybersecurity-and-aml-how-the-twain-must-meet/.

[111] *Id.*

[112] *Id; See also* Clifford Chance PDF (internal citations omitted) (Note that the advisory does not change any of the existing laws).

[113] Kentours, *supra* note 112 at *Id.*

managers in those groups fail to fulfill their duties. As we will see in the next section, this is not the case.

III. THE RULE, INDIVIDUAL CORPORATE LIABILITY, AND SUGGESTIONS

In 2013, the NYDFS conducted a survey on cyber-security.[114] 60 community and regional banks, 12 credit unions, and 82 foreign branches and agencies participated in the NYDFS's questionnaire. The questionnaire asked questions about "each participant's information security framework; corporate governance around cyber security; use and frequency of penetration testing and results; budget and costs associated with cyber security; the frequency, nature, cost of, and response to cyber security breaches; and future plans on cyber security."[115] NYDFS also met with "depository institutions and cybersecurity experts . . . to discuss industry trends, concerns, and opportunities for improvement."[116]

NYDFS's findings discussed management of information technology systems; information security frameworks; use of security technologies; penetration testing; budget and costs; corporate governance; cybersecurity incidents and breaches; and planning for the future.[117] Most institutions experienced intrusions, and the larger the institution, the more likely it was to experience malware and phishing attempts.[118]

It was further noted that larger institutions were more likely to experience financial losses after a cyber-attack.[119] These institutions were also reported to be more likely to have a cybersecurity plan

---

[114] Report on Cyber Security in the Banking Sector, N.Y. DEP'T OF FIN. SERVS. (May 2014), *available at* http://www.dfs.ny.gov/reportpub/dfs_cyber_banking_report_052014.pdf.

[115] *Id.*

[116] *Id.*

[117] *Id.*

[118] *Id.*

[119] *Id.*

instituted than their smaller counterparts.[120] Recent examples help illustrate this last point. In 2011, more than 300,000 Citibank accounts were compromised in a targeted hack.[121] In 2012, a cyber-attack focused on employee login credentials at Bank of America and Wells Fargo.[122]

An April 2015 update on the NYDFS report focused on third-party security service providers, as well as steps taken to implement the U.S. Commerce Department's National Institute of Standards and Technology.[123] Most of the institutions involved had taken or were taking steps to implement NIST principles, but the application of those principles varied across institutions.[124] Ultimately, the report concluded that banks were taking steps to increase cybersecurity, although progress varied depending on an institution's size and type.[125]

On September 13th, 2016, New York Governor Andrew Cuomo announced "first-in-the-nation" regulations to protect New York financial institutions from cyber-attacks.[126] In his remarks, Governor Cuomo said:

"New York, the financial capital of the world, is leading the nation in taking decisive action to our consumers and our financial system from serious economic harm that is often perpetrated by state-sponsored organizations, terrorist networks, and other criminal enterprises. This regulation helps guarantee the financial services

---

120 *Id.*

121 *Banks Likely to Remain Top Cybercrime Targets*, SYMANTEC (last accessed Nov. 30, 2016), *available at* https://www.symantec.com/content/en/us/enterprise/other_resources/b_Financial_Attacks_Exec_Report.pdf. *See also,* Press Release, CitiGroup Inc., Updated Information on Recent Compromise to Citi Account Online for Our Customers, (June 15, 2011), *available at* http://citigroup.com/citi/press/2011/110610c.htm.

122 *Id.*

123 Press Release, NYS Department of Financial Services, *Update on Cyber Security in the Banking Sector: Third Party Service Providers*, NYS DEPARTMENT OF FINANCIAL SERVICES, (April 2015), *available at* http://www.dfs.ny.gov/reportpub/dfs_rpt_tpvendor_042015.pdf [*hereinafter* "2015 Report"].

124 *Id.*

125 *Id.*

126 Governor Cuomo Press Release, *supra* note 8.

industry upholds its obligation to protect consumers and ensure that its systems are sufficiently constructed to prevent cyber-attacks to the fullest extent possible."[127]

The proposed regulation includes proposals designed to balance "certain regulatory minimum standards while maintaining flexibility so that the final rule does not limit industry innovation and instead encourages firms to keep pace with technological advances."[128] Although this article is not intended to provide a thorough analysis of the components contained within either the cyber-security rule, or the AML rule, a brief overview nonetheless provides helpful context in regards to the certification rules.

The cybersecurity program requires every covered entity[129] to establish and maintain a cybersecurity program to ensure confidentiality, integrity, and the availability of its Information Systems,[130] which, among other things, means "a discrete set of electronic information resources organized for the collection, maintenance, use, sharing, dissemination or disposition of electronic information."[131] Covered entities are to implement and maintain a written cybersecurity policy setting forth policies and procedures in order to protect Information Systems and private information stored on those systems. The minimum policy standards require covered entities to address:

1. Information security;

2. Data governance and classification;

3. Access controls and identity management;

---

127 *Id.*

128 *Id.*

129 "[A]ny [individual, partnership, corporation, association, or other entity] operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the banking law, the insurance law, or the financial services law."

130 Press Release, Proposed Regulations: Section 500.00, N.Y. DEP'T FIN. SERVS. (September 2016), *available at* http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf(last accessed Sept. 2016).

131 *Id.*

4. Business continuity and disaster recovery planning and resources;

5. Capacity and performance planning;

6. Systems operations and availability concerns;

7. Systems and network security;

8. Systems and network monitoring;

9. Systems and application development and quality assurance;

10. Physical security and environmental controls;

11. Customer data privacy;

12. Vendor and third-party service provider management;

13. Risk assessment; and

14. Incident response.[132]

This requires the board of directors or an equivalent governing body to review the policy as frequently as necessary (but no less frequently than annually), and a senior officer to approve of the policy's contents.[133]

The proposed regulation also contained an annual certification of compliance requirement.[134] Every covered entity[135] must certify that it follows the requirements of the regulation.[136] The

---

[132] *Id.*

[133] *Id.*

[134] Press Release, Maria T. Vullo, Notice of Final Regulations' Promulgation under Part 500 Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York: Cybersecurity Requirements for Financial Services Companies, 500.17(b), (Feb. 13, 2017), *available at* http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf.

[135] *Id.*

[136] *Id.*

language of the certification is found in Appendix A and reads as follows:

> The Board of Directors or a Senior Officer of the Covered Entity certifies:
>
> (1) The Board of Directors (or name of Senior Officer(s)) have reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary;
>
> To the best of the (Board of Directors) or (name of Senior Officer(s)) knowledge, the Cybersecurity Program of (name of Covered Entity as of ___ (date of the Board Resolution or Senior Officer(s) Compliance Finding) for the year ended ____ (year for which Board Resolution or Compliance Finding is provided) complies with Part __.
>
> Signed [and dated] by the Chairperson of the Board of Directors or Senior Officer(s).
>
> Failure to certify will be enforced under "any applicable laws," including civil and criminal penalties.[137]

NYDFS's final cybersecurity regulations went into effect March 1st, 2017.[138] In a February 16, 2017 press release, New York Governor Andrew M. Cuomo said:

---

[137] *Id.*; *see also* PwC, *AML monitoring: New York regulator gets prescriptive*, FINANCIAL CRIMES OBSERVER PWC, (July 2016), *available at* http://www.pwc.com/us/en/financial-services/financial-crimes/publications/assets/aml-monitoring-nydfs-2016.pdf [*hereinafter* "PwC"].

[138] Press Release, Governor Cuomo, Governor Cuomo Announces First-in-the-Nation Cybersecurity Regulation Protecting Consumers and Financial Institutions from Cyber-Attacks to Take Effect March 1, (February 16, 2017), *available at* http://www.dfs.ny.gov/about/press/pr1702161.htm.

> New York is the financial capital of the world, and it is critical that we do everything in our power to protect consumers and our financial system from the ever increasing threat of cyber-attacks . . . These strong, first-in-the-nation protections will help ensure this industry has the necessary safeguards in place in order to protect themselves and the New Yorkers they serve from the serious economic harm caused by these devastating cyber-crimes.[139]

The final regulation includes

- Controls relating to the governance framework for a robust cybersecurity program including requirements for a program that is adequately funded and staffed, overseen by qualified management, and reported on periodically to the most senior governing body of the organization;

- Risk-based minimum standards for technology systems including access controls, data protection including encryption, and penetration testing;

- Required minimum standards to help address any cyber breaches including an incident response plan, preservation of data to respond to such breaches, and notice to DFS of material events; and

- Accountability by requiring identification and documentation of material deficiencies, remediation plans and annual certifications of regulatory compliance to DFS.[140]

Section 500.20, which covers enforcement, says that "This regulation will be enforced by the superintendent pursuant to, and is

139 *Id.*
140 *Id.*

not intended to limit, the superintendent's authority under any applicable laws."[141]

So far - so good. However, in June 2016, NYDFS had issued a similar final rule regarding AML compliance certification.[142] This issuance was a result of multiple NYDFS investigations into compliance at "regulated institutions" ("all banks, trust companies, private bankers, savings banks and savings and loans associations chartered under New York Banking Law, New York-licensed branches and agencies of foreign banking corporations, as well as New York-licensed check cashiers and money transmitters[]"[143]) with applicable money laundering rules.[144] The investigation identified shortcomings in these financial institution's transaction monitoring and filtering programs, which was in turn attributable to a lack of governance, oversight, and accountability at senior levels.[145] Based on this investigation and other factors, NYDFS believed financial institutions had systemic shortcomings in their AML programs and wanted to not only clarify AML program requirements, but also have the Board of Directors or a Senior Officer submit a Board Resolution or Compliance Finding.[146]

The final AML rules require every regulated institution to maintain a Transaction Monitoring Program that should contain, where applicable, the following attributes:

1. Based on the institution's Risk Assessment;

---

141 *Supra* note 10.

142 Publication, Shearman & Sterling LLP, *NYS Department of Financial Services Outlines Requirements for Transaction Monitoring and Filtering Programs of NY State-Licensed Institutions*, SHEARMAN & STERLING LLP CLIENT PUBLICATIONS (Jul. 20, 2016), *available at* http://www.shearman.com/~/media/Files/NewsInsights/Publications/2016/07/NYS-Department-of-Financial-Services-Outlines-Requirements-FIAFR-072016.pdf [*hereinafter* "Shearman and Sterling"].

143 *Id.*

144 *Id.*

145 *Id.*

146 *Id.*

2. Periodically reviewed and updated to reflect and account for changes to BSA/AML laws and other relevant information;

3. Match BSA/AML risks to the firm's business, product and service lines, and customers;

4. BSA/AML detection scenarios with values and amounts that detect potential money laundering, suspicious activity, or other illegal activity;

5. A full scope testing of the Transaction Monitoring Program, including governance review, data mapping, transaction coding, detection scenario logic, model validation, data input and Program output;

6. Documentation articulating the institution's current detection scenarios and the assumptions, thresholds, and parameters of those scenarios;

7. Protocols outlining how the firm will investigate the Transaction Monitoring Program's alerts, how the Regulated Institution will decide which alerts will result in a filing or other action, who is responsible for deciding, and how the investigative and decision-making process is to be documented; and

8. Be subject to on-going analysis in order to determine whether detection scenarios, underlying rules, threshold values, parameters, and assumptions are still relevant.[147]

The Regulated Institution's Filtering Program's requirements are similar to the Monitoring Program in that they are only to be implemented where applicable, and are as follows:

1. Be based on the institution's Risk Assessment;

147 *Id.*

2. Be based on technology, processes, or tools that will match names and accounts consistent with the institution's risks, transaction, and product profiles;

3. Full scope testing of the Filtering Program, including relevant reviews of data matching, determining whether the OFAC sanctions list and threshold settings synchronize to an institution's risks; assessing the logical fit of technology or tools, model validation, and data input with the Program's output;

4. On-going analysis to assess technology and tool's logic and performance in matching names and accounts, as well as the OFAC sanctions list and threshold settings to see if they map the institution's risks, and

5. Documentation articulating the Filtering Program's intent and design for tools, processes, and technology.[148]

Both the Transaction Monitoring and Filtering Programs are required to have, where applicable:

1. ID of all data sources with relevant data;

2. Validation of data's accuracy, integrity, and quality, ensuring accurate and complete data flows through the Transaction Monitoring and Filtering Program;

3. Processes for data extraction and loading to ensure a complete and accurate data transfer from source to system (provided automated systems are used)

4. Governance and management oversight, including policies and procedures that govern changes to the Transaction Monitoring and Filtering Program ensuring that changes are managed, reported, audited, defined, and controlled;

---

[148] *Id.*

5. Vendor selection processes where third-party vendors are used in the Transaction Monitoring and Filtering Program;

6. Funding for the Transaction Monitoring and Filtering Program;

7. Qualified personnel or third-party consultants responsible for various aspects of the Transaction Monitoring and Filtering Program, including design, implementation, ongoing analysis, planning, operation testing, and

8. Periodic training of all Transaction Monitoring and Filtering Program stakeholders.[149]

When Regulated Institutions identify areas, systems, or processes needing material improvements, updates, or redesigns, the Regulated Institutions are required to document the identifications made, and the corresponding planned remedial efforts. The Superintendent of NYDFS must be able to view these documents.[150]

Either the board or the senior officers of a company must certify that the company has followed these rules outlined above. The Board Resolution or Compliance Finding requirement dictates that:

> [E]ach Regulated Institution "shall adopt and submit to the Superintendent a Board Resolution or Senior Officer(s) Compliance Finding in the form set forth in Attachment A by April 15th of each year. Each Regulated Institution shall maintain for examination by the Department all records, schedules and data supporting adoption of the Board Resolution or

[149] *Id.*
[150] *Id.*

> Senior Officer(s) Compliance Finding for a period of five years.[151]

The language of the aforementioned certification is as follows:

> The Board of Directors (or name of Senior Officer(s)) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary to adopt this Board Resolution or Senior Officer Compliance Finding.
>
> The Board of Directors or Senior Officer(s) has taken all steps necessary to confirm that (name of Regulated Institution) as of ___ (date of the Board Resolution or Senior Officer(s) Compliance Finding) for the year ended ___ (year for which Board Resolution or Compliance Finding is provided) complies with [Transaction Monitoring and Filtering Requirements].
>
> Signed [and dated] by each member of the Board of Directors or Senior Officer(s).[152]

In the final rule, these requirements are to "be enforced pursuant to, and is not intended to limit, the Superintendent's authority under any applicable laws."[153] Thus, the scope of the Superintendent's authority is both civil and criminal. However, the original wording of the rule was harsh, as illustrated below:

> All Regulated Institutions shall be subject to all applicable penalties provided for by the Banking Law and the Financial Services Law for failure to maintain a Transaction Monitoring Program, or a Watch List

---

[151] *Id.*

[152] Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications, 3 N.Y.C.R.R. Part 504 (Mar. 2017), *available at* http://docs.dos.ny.gov/info/register/2016/july20/pdf/rulemaking.pdf *and* http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp504t.pdf.

[153] Shearman and Sterling, *supra* note 142.

> Filtering Program complying with the requirements of this Part and or failure to file the Certifications required under Section 504.4 hereof. A Certifying Senior Officer who files an incorrect or false Annual Certification also may be subject to criminal penalties for such filing.[154]

It is unclear why the original language was worded as it was. More than likely, the language intended to serve two purposes: (1) to underline the seriousness of the offense, and (2) to warn potential officers certifying the Annual Certification of the consequences resulting from a failure to certify the company's program.

Regardless, due to industry feedback that language was struck out entirely and replaced with new language for the finalized rule. In the final rule, NYDFS removed the threat of criminal penalties for incorrect or falsified filings.[155]

Thus, there are meaningful distinctions between the requirements of the cybersecurity rule and the AML rule. However, the reality of modern financial institutions means that AML is a significant component of cybersecurity, such that AML measures cannot be effective without cybersecurity, and cybersecurity in financial institutions cannot be fully effective without AML measures. In the following section, I will explain why the current rules require some form of harmonization in their application and enforcement, and further, why those rules need to establish a specific standard for the imposition of criminal liability in specific instances.

IV. SUGGESTIONS AND RATIONALE

Both the cybersecurity rules and the AML rules should have the same language, however, they do not. Unfortunately, both rules lack much-needed language allowing for the imposition of criminal liability in appropriate situations. This problem could be addressed

---

154 *Id.*

155 PwC, *supra* note 137.

through a number of ways and considerations. First, one must consider that by softening the language in both rules, the NYDFS was not responsive to institutions' vocalized concerns, and likely only further confused individuals trying to comply. Second, if both rules contain the same language, the possibility of corporate directors avoiding liability in one function, while negating liability in another for the same act, will likely lessen. Third, by emphasizing the potential of corporate criminal liability the rule will more properly reflect the principles outlined by the Yates memorandum. Even though the Yates memorandum is not an official policy of the New York Attorney General's Office, aligning the language of the rules with the spirit of the Yates memorandum could eliminate the complexity created by the current compliance rules for company directors.

A. Changing the Language of the Statute but not the Underlying Enforcement Mechanism is Unresponsive to Concerns and Only Confuses Firms Trying to Comply with the Rule

In response to public comments regarding the rule, the NYSFDS changed the AML rule's language so that the regulation "[would] be enforced pursuant to, and [] not intended to limit, the Superintendent's authority under any applicable laws."[156] Although the laws are not explicitly mentioned, the language of the AML rule presumably refers to legislation relating to Banking, Insurance, and Financial law. However, if this is true, the NYSFDS is committing two errors.

First, by not changing the underlying penalties of the law, the NYSFDS is not being responsive enough to the concerns of commenters. Secondly, by stating only that regulators will pursue enforcement under "any and all applicable laws," individuals are left "in the dark" about specific applicable law. If we were to assume that a law's ability to be interpreted directly influences the law's likelihood of being followed, then one must also consider the vagueness of this rule and its resultant effect on compliance.

---

156 Shearman and Sterling, *supra* note 142.

This problem of vagueness in compliance can also be found in the proposed cybersecurity rule. Like the AML rule, the cybersecurity rule only states that the Superintendent will enforce the Regulation pursuant to "authority under any applicable laws."[157] One can only speculate why the rule is phrased this way. Perhaps this phraseology was a response to the public comment regarding the AML rules and was intended to preemptively address similar complaints about the AML rule. Again, however, this language is ineffective at best and counterproductive at worst. This lack of clarity could feasibly hinder corporations from ensuring which laws are applicable, and consequently, what standards to adhere to when certifying their cybersecurity programs.

Furthermore, rule-makers determined that the prior language was not precise enough to warrant inclusion. As we have seen, cybersecurity breaches and AML risks are frequent. Thus, this arguably makes individual penalization through criminal liability unjust in certain situations, such as, for example, the filing of false or incorrect Annual Certifications in good faith. Beyond that, a variety of scenarios could occur: firms may have to start offering large salaries to compliance officers just to attract quality talent, or, firms may feel encouraged to structure their company in such a way that does not require a New York state business charter, and thus bypassing the rule. In a true nightmare scenario, firms could just dissolve their charters, leave New York, and set up shop in alternative financial centers such as San Francisco, Boston, Chicago, Charlotte, or Washington, D.C.

B. Uniform Language as a Response to Dual Corporate Officer Liability Loopholes

As the rules are currently written, it is entirely possible that an individual could face criminal liability for a certification violation in the cybersecurity context, yet simultaneously avoid criminal liability under the AML rules. To be sure, in some situations this will not be relevant. For example, suppose that there is a cybersecurity breach of

---

157 Vullo, *supra* note 134.

a financial institution based on corporate espionage. If, after an individual makes a bad faith cybersecurity certification, a hacker gets into an employee's email, he may learn of a new marketing campaign, the valuation of a confidential M&A deal, or proprietary research created by a firm's research team. Cybersecurity breaches involving financial institutions are often related to some form of money laundering activity. Such breaches are cybersecurity breaches, although they do not involve the laundering of money.

However, in situations where a cybersecurity breach does involve money laundering, if both the cybersecurity policy and money laundering policy were certified by an individual omission or outright lie, it is possible that the individual could avoid liability under the AML rule, but not the cybersecurity rule. A predictable argument could be that criminal prosecution under the AML rule is unfair because the language change from the proposed rule to the final rule reflects a retraction in the intended harshness of the policy against criminal prosecution. Thus, it is foreseeable that criminal liability was not intended to be permissible for AML violations, and the rule is thus arguably be unconstitutional for being overly vague.

However, if both rules were to have the exact same language, two results would occur. First, loopholes are no longer present in those situations where both rules apply, but with contrasting language. Second, assuming all elements are met, it would be difficult, if not impossible, for an individual to argue that it was unclear whether their failure to comply with the certification mechanism would allow for criminal liability sanctions.

C. The Yates Memorandum & Creating a Comprehensive Model

Having a rule that reflects the Yates memorandum not only makes the rule easier to follow, but also sets good precedent for further states' adoption and implementation. Responding to industry concerns, eliminating the possibility of loopholes, and creating precise language are key aspects of the new language. The next and final element is that the new language should reflect the tenor of the Yates memorandum, such that it makes the rule easier to follow, but

also sets a good precedent for other states to copy should they choose to implement their own state policies.

Again, it bears repeating that the Yates memorandum, technically, has no bearing on the New York Attorney General's Office or the NYDFS. After all, the Yates memorandum is part of the DOJ, and thus reflects federal policy. However, many New York banks have not worked solely within the confines of New York for quite some time: indeed, it is hard to recall when New York banks operated solely within the United States. Goldman Sachs, JPMorgan and Deutsche Bank are just a few New York chartered organizations with international reach.[158] As such, in their operations these institutions are subject to not just New York law, but federal law as well. Despite New York's outsized influence within the financial sector, common practice for these organizations is to channel their resources towards federal law compliance.

There is another advantage to this. By making the rule reflective of the Yates memorandum and easier to follow, it removes an incentive for an organization to move its banking charter from New York to another state with more relaxed banking standards.

V. THE NEW RULE

If the current language and the proposed language of both the cybersecurity and AML certification policies are not adequate, then what is? This author proposes the following rules for the cybersecurity and AML programs, respectively. For cybersecurity:

All Regulated Institutions shall be subject to all applicable penalties provided for by the Banking Law and the Financial Services Law for failure to maintain a cybersecurity program complying with the requirements of this Part and or failure to file the Certifications required under Section 500.17 hereof. A Certifying Senior Officer

[158] *See generally* Report, New York State Chartered Institutions as of December 31, 2012, N.Y. DEP'T FIN. SERVS. (Dec. 31, 2012), *available at* http://www.dfs.ny.gov/reportpub/annual/annualbanklist.htm.

who *intentionally*, *knowingly*, or *recklessly* files an incorrect or false Annual Certification also may be subject to criminal penalties for such filing.

Then, for the AML:

All Regulated Institutions shall be subject to all applicable penalties provided for by the Banking Law and the Financial Services Law for failure to maintain a Transaction Monitoring Program, or a Watch List Filtering Program complying with the requirements of this Part and or failure to file the Certifications required under Section 504.4 hereof. A Certifying Senior Officer who *intentionally*, *knowingly*, or *recklessly* files an incorrect or false Annual Certification also may be subject to criminal penalties for such filing.

This proposed language achieves two purposes. First, by giving explicit standards, the language makes clear that a criminal enforcement will only be triggered where an individual's behavior manifests a level of intent beyond mere negligence. The *Haider* case, described *supra*, provides a clear example of when an individual director's failure to provide adequate internal controls was a result of mere negligence. As illustrated by the *Haider* case, it would be unfair to punish all individuals for negligence or strict liability offenses and could lead to unintended consequences in an industry where complete prevention has proven impossible. Second, and relatedly, this proposed rule reflects the reality that AML and cybersecurity divisions at certain financial institutions face extraordinary difficulties and overlapping functions. The proposed rule is narrowly tailored to prevent the behavior seen in *Haider*, or rather, violations conducted by individuals intentionally, knowingly, or recklessly; but not the behavior of otherwise good-faith individuals who mistakenly certify a compliance program. Distinguishing between negligent and reckless conduct may be difficult at times, but nonetheless, this proposed rule provides a minimum standard and guide for enforcement agencies to adhere to.

VI. CONCLUSION

AML and cybersecurity are separate policies, yet, closely intertwined and critical as a defense for financial institutions. These institutions are constantly under attack from outsiders, and unfortunately, bound to fall victim to a breach at some point. After all, even if 10,000 attacks occur and 9,999 of them fail, all it takes is one; hackers may still be successful in damaging a targeted institution, even when the breach is minimally intrusive.

The New York State Department of Financial Services made a mistake in weakening the language of its proposed rules. The NYDFS was not responsive to industry concerns and the rules were not written clearly enough to meaningfully advise parties affected by the consequences of a failure to comply. By strengthening the language so that clear consequences are understood and established, and by setting a clear standard of what will trigger potential criminal liability, this Author's proposed language will serve the dual purpose of reassuring individuals at firms of what actions would impose criminal liability, and would further ensure the New York State Department of Financial Services that its goal of increasing cybersecurity and AML regulations has been met.

Penn State
Journal of Law & International Affairs

2017 VOLUME 5 NO. 1

THE INNOCENT COMBATANT: PRESERVING THEIR *JUS IN BELLO* PROTECTIONS

Mark "Max" Maxwell and Richard V. Meyer***

* Mark "Max" Maxwell was a military attorney (Judge Advocate) for nearly 25 years. He currently serves as the Deputy Legal Counsel for U.S. Africa Command. Max is a graduate of Duke University, the University of North Carolina School of Law, and the National War College. *The content of this article in no way reflects the opinion of the U.S. Government or the U.S. Department of Defense*.

** Professor Richard V. Meyer is the Director of International & LL.M. Programs at the Mississippi College School of Law. A retired judge advocate, Meyer's final military assignment was as an Associate Professor at the United States Military Academy at West Point and was subsequently appointed as a Senior Fellow for the West Point Center for the Rule of Law. He serves as the Chair of the International Committee for the Southeastern Association of Law Schools and on the editorial committee of Oxford's Journal of International Criminal Justice. He has Masters of Law degrees from Columbia and the Judge Advocate General's School and a *Juris Doctor* from Northern Illinois University.

TABLE OF CONTENTS

I. INTRODUCTION

On September 4th, 2014, Officer Sean Groubert of the South Carolina State Police pulled his police cruiser behind the vehicle driven by Levar Jones at a gas station in South Carolina. Officer Jones would later state the reason he pulled behind Jones was because he observed Jones was not wearing his seat belt. Jones would later state he removed his seat belt upon pulling into the gas station to exit his vehicle and enter the station. All of the following events were captured by the dash-cam in Officer Groubert's car.[1]

Levar Jones exited his vehicle and, with his car door still open, noticed the police vehicle behind him. His face exhibited surprise and confusion.[2] Officer Groubert requested Jones' license in a controlled speaking voice.[3] Jones pats his pocket, and realizing his wallet is not there, does a rapid shoulder shift from facing Groubert to facing the inside of his vehicle.[4] He then leans into the vehicle as an ordinary place to secure his wallet, which he had left sitting on the front seat.[5] However, Officer Groubert (apparently) viewed the rapid shoulder shift as an aggressive and hostile act. In the next three seconds of film, he shouts "Get out of the Car!" twice, runs to cover behind Jones' vehicle and fires four shouts at Jones.[6] The first shot hits Jones while he is turning around with the wallet in his hand. He drops the wallet and backs away from the officer while putting his hands up while three more shots hit him. In the same dash-cam video, Groubert later describes the events to his supervisor.[7] Groubert describes Jones' surprise and confusion as an act of "staring him down"; Jones' leaning into his vehicle to secure his

---

[1] This video can be found in many places on the internet. The one we will reference is available at: The State Newspaper, *Sept 4 Groubert traffic* stop, YOUTUBE (Sept. 24, 2014), https://m.youtube.com/watch?v=RBUUO_VFYMs.

[2] *Id.* at time stamp :40.

[3] *Id.* at time stamp :42.

[4] *Id.* at time stamp :43 - :44.

[5] *Id.* at time stamp :45.

[6] *Id.* at time stamp :46 - :49.

[7] This longer video can be found at: Tony Santaella and Steven Dial, *Trooper on Shooting: 'He Kept Coming Towards Me'*, WLTX19 (Sept. 27, 2014), http://www.wltx.com/story/news/local/2014/09/26/sean-groubert-gives-his-account-of-shooting-levar-jones/16295527/ (last visited Jan. 3, 2017).

wallet as an act of "diving into his vehicle"; Jones' acts of walking backwards while putting his hands up as "he kept coming at me"; and Jones' wallet as a perceived weapon.[8]

On the one hand we could assume these to be self-serving and dishonest statements by Officer Groubert. This assumption is not necessary and it is far more probative to view them as the honest (mis)perception of a shooter in a perceived hostile environment. Under that lens, Groubert's statements reflect a perception of an African American male as a potential hostile in an asymmetric battlefield-like environment,[9] and give a rare insight into a shooter's psyche – a rapid, stress-filled situation.

The landscape of modern asymmetric conflicts, such as the war in Afghanistan, is also murky. The Soldier, like the police officer, is burdened with the reality that he does not know who the bad guy is and who the innocent is. But the rules governing the Soldier are starkly different than those governing the police officer for sound and logical reasons. In a *New York Times* editorial, U.S. Marine Corps Captain Timothy Kudo discusses his own use of force in Afghanistan.[10] While a commander, he was asked permission by his Marines to kill two Afghans: "The voice on the other end of the radio said: 'There are two people digging by the side of the road. Can we shoot them?'" The presumption is the two were implanting an improvised explosion device – known as an IED – to kill or injure Afghan or coalition Soldiers. Captain Kudo gave permission and the two diggers were killed.[11] There was an ever-present possibility the diggers were merely irrigating their farm land and not sowing seeds of violence toward Captain Kudo, his Marines, and the Afghan State.

---

[8] *Id.*

[9] The attitude of police in the United States towards African American males has been the subject of much commentary and literature and is not the subject of this piece. We mention it as a basis of comparison to the view of Soldiers towards potential threats in the modern asymmetric battlefield.

[10] Timothy Kudo, Editorial, *How We Learned to Kill*, N.Y. TIMES, Mar. 1, 2015, New York Edition at SR1.

[11] *Id.*

How we assess the use of force and whether force is appropriate in any given situation is instrumental to how we function as a deliberative democracy. While we might all agree Officer Groubert's actions are reprehensible and probably criminal, Captain Kudo's are less open to clear judgment. Should the judgment depend on whether Captain Kudo was ultimately correct; that is, the diggers were, in fact, bad guys, rather than innocent farmers making a living? If Levar Jones had held up a gun rather than a wallet upon exiting his vehicle, the authorities would probably have viewed Officer Groubert's actions differently. But the true (rather than perceived) battlefield is a significantly different legal reality where far greater uses of force have been permitted, including knowingly causing the death of innocents.[12] Evaluating Captain Kudo's actions is made problematic by the blending of warfighting with peacekeeping and even battlefield law enforcement mandated by asymmetric warfare.

Among the volumes written on when force can be exercised by Soldiers during armed conflict in the name of the State, the trend over the last century has been to curtail a Soldier's use of force and rightfully so. The adoption by virtually every State[13] of The Hague Conventions in 1907,[14] the Geneva Conventions[15] in the wake of World War II, along with their Protocols in 1977,[16] has been with a

---

[12] Under the concept of proportionality, lawful combatants can knowingly cause the incidental death of innocent noncombatants if the military advantage gained exceeds their loss. *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. 52, June 8, 1977, 1125 U.N.T.S. 3 [*hereinafter* Additional Protocol I].

[13] The International Committee of the Red Cross [*hereinafter* "ICRC"] tracks the current signatories to the Geneva Conventions and their Additional Protocols at https://www.icrc.org/en/war-and-law/treaties-customary-law/geneva-conventions (The Geneva Conventions of 1949 have been ratified by every member state of the United Nations).

[14] Convention Respecting the Laws and Customs of War on Land, 36 Stat. 2277, October 18, 1907.

[15] Jean S. Pictet, *The New Geneva Conventions for the Protection of War Victims*, 45 AM. J. INT'L. L. 462 (1951).

[16] Additional Protocol I and Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), June 8, 1977, 1125 U.N.T.S. 609 [*hereinafter "*Additional Protocol II"].

singular purpose: to limit the devastation inflicted by armed conflict. Armed conflict, however, persists. Whether it is the war in Afghanistan or the crisis in the Ukraine, bloodshed of both innocent civilians and lawful combatants/privileged belligerents[17] is a persistent reality. In the modern era, complicating the calculus of how to limit the destruction of war, many of these armed conflicts are fueled by actors who refuse to wear military uniforms, carry their arms openly, and become privileged belligerents; these actors lurk amongst civilians and never show their true intent until they strike.

In the last decade, the trajectory of some courts, academics, and even military leaders of States[18] is to limit the force States' militaries can use during conflict. The intent of these limits on what force, including lethal force, militaries can use to accomplish the mission is quite noble. The logic is the less force used by a Soldier, the less death and destruction inflicted upon innocents. However, these limitations are tainted by misunderstandings and mistakes concerning the principles and goals of the Just War Theory, particularly in the evaluation of battlefield conduct: *jus in bello*.

Academics and jurists have extrapolated familiar concepts from criminal law jurisprudence, those used to evaluate Officer Groubert's conduct, such as intent, necessity, and proportionality, and attempted to apply them to evaluate the acts of the privileged belligerent.[19] The attempt to make the dissimilar into the similar is understandable because man habitually tries to characterize the unfamiliar by extrapolating from a familiar paradigm. However, while the same terms may be used,[20] the meaning of those terms differ

---

[17] "The term "privileged belligerent" means an individual belonging to one of the eight categories enumerated in Article 4 of the Geneva Convention Relative to the Treatment of Prisoners of War. 10 U.S.C. § 948a(6).

[18] Examples of each are discussed later in this chapter.

[19] *See* GEORGE P. FLETCHER & JENS DAVID OHLIN, DEFENDING HUMANITY: WHEN FORCE IS JUSTIFIED AND WHY (Oxford: Oxford Univ. Press, 2008) [*hereinafter* "Defending Humanity"] for an extrapolation of criminal law concepts to *jus ad bellum*, an extrapolation that makes much more sense than to *jus in bello*.

[20] Both the criminal law and the *jus in bello* paradigms include common terms such as self-defense and necessity, but the meanings can vary significantly.

significantly between law enforcement and war.[21] This extrapolation manifests itself in applying human rights law norms and the universal reach of an individual's right to life. Criminal law exists to preserve the peace, whereas *jus in bello* works to end conflict.[22]

Exacerbating the problem is the other half of the Just War Theory, *jus ad bellum. Jus ad bellum is a set of international principles* regulating when the State can initiate armed conflict. Extrapolating criminal law jurisprudence to evaluate *jus ad bellum* actions is rational because the goals and core concepts of the two paradigms are nearly identical:[23] In both systems, the "citizens" (individuals in criminal law, States in *jus ad bellum*) lose the ability to use violence to achieve their aims except in rare circumstances where the violence is legally authorized (law enforcement and U.N. Security Council Resolution) or justified (self-defense of the individual and the state). Further, both share a common fundamental goal: preserving the peace. Therefore, using criminal law concepts and jurisprudence to evaluate *jus ad bellum* action, as proposed by George Fletcher and Jens Ohlin in *Defending Humanity*, is proper.[24] The reason: the words *and meaning* are the same. What is not defensible, morally or legally, is using this similarity as a gateway to then apply criminal law concepts to *jus in bello* where these substantive and goal similarities do not exist. The words may be the same, but the meaning is different.

---

[21] A good example of this divergence is the concept of self-defense. In the criminal law paradigm, the individual's right of self-defense is limited by, among other things, the responsibility to not cause the death of anyone but the aggressor, and the ability to use force in self-defense is limited to the timeframe of the aggression. In contrast, on the battlefield, a lawful combatant can knowingly cause the death of an innocent in self-defense, provided the death is incidental and that it is exceeded by the military advantage of staying alive. Further, the lawful combatant can engage in status rather than conduct based self-defense.

[22] "The object of war has been understood to be the submission of the enemy as quickly and efficiently as possible." The Department of DOD LAW OF WAR MANUAL, June 2015, [*hereinafter* "DOD LAW OF WAR MANUAL"] paragraph 1.4.1 citing 1940 RULES OF LAND WARFARE ¶22 ("The object of war is to bring about the complete submission of the enemy as soon as possible by means of regulated violence."); 1914 RULES OF LAND WARFARE ¶10 (same).

[23] *Id.*

[24] *Id.*

This extrapolation of criminal law concepts to the battlefield is not defensible because in armed conflict a commander's calculus revolves around military necessity--defined as "the necessity of those measures which are indispensable for securing the ends of the war, and which are lawful according to the modern law and usages of war."[25] The commander must balance, on one hand, the necessary precautions to protect civilians with, on the other hand, the commander's conclusion of military necessity. Imbedded in this conclusion is military judgment. This concept simply does not exist in domestic criminal law. And with any judgment, especially one which stems from whether necessary precautions were taken in light of the military action in the name of military necessity, there is the element of subjectivity. The modern trend has been to extend "the domestic law of negligence to the battle zone – where civilian norms of duty of care" are applied to military decisions.[26] This means civilian criminal standards are being applied to decisions made in war. The manifestation of this trend is to focus on the results of the military decision after the fact (*e.g.*, were civilians killed?), rather than focus on the rationale of the military act under current International Humanitarian Law (IHL).[27]

Conflating civilian criminal standards with the rationale of a military act under IHL comes at a high cost for democratic armies and has, in these authors' opinion, not been fully debated. The biggest cost is to the effectiveness of a State's military to bring an end to armed conflict. Efforts to protect the enemy belligerent and innocent civilians by limiting the Soldier's lethality acts to defeat a

---

[25] DOD LAW OF WAR MANUAL paragraph 2.2.1 citing, among multiple other sources, General Order No. 100, the Instructions for the Government of Armies of the United States in the Field, commonly known as the Lieber Code art. 14 ("Military necessity, as understood by modern civilized nations, consists in the necessity of those measures which are indispensable for securing the ends of the war, and which are lawful according to the modern law and usages of war.").

[26] Thomas Tugendhat & Laura Croft, *The Fog of Law: An Introduction to the Legal Erosion of British Fighting Power,* Policy Exchange (2013) at 11, https://policyexchange.org.uk/wp-content/uploads/2016/09/the-fog-of-law.pdf (last visited Mar. 31, 2017).

[27] International Humanitarian Law is synonymous with the Law of War and the Law of Armed Conflict. This body of international law regulates the conduct of forces when engaged in war and armed conflict.

fundamental goal of *jus in bello*, bringing about an end to the war; therefore causing an increase, rather than decrease, of violence.

Unrealistic limitations on the Soldier means there are rules he can never overcome. If the acid test is to kill no civilians, for example, then closing with and killing or capturing an amorphous enemy who looks and acts like a civilian is profoundly difficult, if not impossible. Placing limitations on the Soldier limits their ability to exercise the principle of military necessity and, therefore, defeats one of the core principles of the Just War Theory.

This article will argue the right of the Soldier to engage and destroy military objectives is inherent to warfare; efforts to stem or limit this force need to be fully understood and carefully considered within *jus in bello* instead of the criminal law paradigm. Failure to do so may actually increase violence rather than decrease it, as well as violate the State's sacred obligation to its designated belligerents: Soldiers.

Even though the Soldier is legally and morally blameless for his presence on the battlefield, he loses the protections of the civilian criminal law against violence. In exchange for this sacrifice, the Soldier gains the right to use violence to execute the mission and bring about an end to the war. Forcing the Soldier to waive his right to the protections of the law while simultaneously denying him the ability to effectively accomplish his mission reduces him to nothing more than a designated target for those who oppose his State.

This article will start with a brief introduction to the core principles of the Just War Theory and use these to identify its fundamental goals. This section will examine the differences between privileged belligerents and civilians and highlight why the rights of privileged belligerents cannot tether to the concepts or goals of domestic criminal law. The second part of the article will then examine five specific trends which are part and parcel to the pervasive wave against the use of force and the actual or potential cost to how Soldiers behave in conflict; that is, *jus in bello*. The authors will ultimately conclude that until war itself is fully eliminated from the human experience, the *lex specialis* of *jus in bello* within the Just War Theory is pragmatically justified and a morally mandated

duty of the international community of States to privileged belligerents.

II. A BRIEF INTRODUCTION OF THE JUST WAR THEORY AND A COMPARISON TO TRADITIONAL CRIMINAL LAW

The Just War Theory has traditionally[28] been divided into the morality of a State or group's decision to engage in armed conflict, *jus ad bellum*, and the manner in which armed conflict is conducted, *jus in bello*.[29]

Jus ad bellum has evolved from the right of states to use war to achieve political ends, enforce treaties, and in reprisal, to the far more restrictive modern approach of Article 2(4) of the United Nations Charter, which requires States to "…refrain from the threat or use of force against .. any state" in order to "…maintain international peace and security."[30] The only commonly recognized exceptions to this prohibition are the use of force authorized by the Security Council[31] and the use of force in self-defense under Article 51[32] of the same charter. In this regard, *jus ad bellum* mirrors the paradigm of civilian criminal law in both goal (preserving peace) and substance (the

[28] Modern academics have posited a third area of concern within the Just War Theory, that of *jus post bellum*, or the responsibility of belligerent states after the conclusion of armed conflict.

[29] MICHAEL WALZER, JUST AND UNJUST WARS: A MORAL ARGUMENT WITH HISTORICAL ILLUSTRATIONS 21 (Basic Books, 3RD ed. 2000) [*hereinafter* "Walzer"]: "War is always judged twice, first with reference to the reasons states have for fighting, secondly with reference to the means they adopt. The first kind of judgment is adjectival in character: we say that a particular war is just or unjust. The second is adverbial: we say that a war is being fought justly or unjustly."

[30] Charter of the United Nations, Jun. 26, 1945, 59 Stat. 1031 article 2(4) [*hereinafter* "UN Charter"].

[31] *Id.* at article 24(2) "The specific powers granted to the Security Council for the discharge of these duties are laid down in Chapters VI, VII, VIII, and XII." These powers include the ability to use force for Chapter VI peacekeeping, or Chapter VII peace enforcement.

[32] *Id.* at article 51 "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."

individual's ability to use force is limited to situations justified by an external imminent threat).

A. The Uniqueness of *Jus in bello*

Unlike *jus ad bellum*, which evolved almost entirely based on international agreement,[33] *jus in bello* is primarily the product of custom. Modern treaties, such as the four Geneva Conventions and its Protocols, have acted to codify rules evolved from core principles developed by the practice of professional warfighters over centuries.[34] These principles include Distinction, Military Necessity, and Proportionality.

1. *The Principle of Distinction.*[35]

Any analysis of *jus in bello* should begin with the principle of distinction, because it is the springing condition for the *lex specialis*. Said another way, without the application of the principle of distinction, the substance of traditional criminal law is an entirely adequate tool to determine the legality of a given act. The principle subdivides into: A) the responsibility of combatants to distinguish themselves from civilians; and B) the responsibility to target only enemy combatants and military objectives with attacks.[36]

---

[33] Prior to its conclusion in the U.N. Charter, the International Military Tribunal at Nuremburg identified the Kellogg-Briand Pact of 1929 as a source of restrictions on the power of *jus ad bellumjus ad bellum* for signees.

[34] The Lieber Code is often cited as the first documentation of the modern laws of war. This code was not a creative work, but rather the result of Francis Lieber working on a committee of military professionals to codify existing customary practice that had been developed over centuries.

[35] DOD LAW OF WAR MANUAL paragraph 2.5.

[36] *Id.*

(i) The Responsibility of Combatants to Distinguish Themselves from Civilians.

International law grants combatants the legal and moral authority to commit violent acts that would otherwise be abhorrent and punishable under traditional criminal law.[37] This privileged belligerency allows them to shoot and kill enemy Soldiers based on their mere status as members of the enemy military force.[38] Criminal law would only allow this attack if properly imposing a death sentence on the victim[39] or if the victim was posing an imminent threat to the shooter (or another) and the shot was a proportional response to that threat[40] (e.g., without a current imminent threat, Officer Groubert could not shoot Levar Jones even if Jones was the worst criminal in history).

Further, except in the case of a death sentence and in preventing the escape of an individual who poses a significant threat of death or serious bodily harm to the officer or others,[41] law enforcement officers have no greater privilege to use deadly force than an ordinary citizen. The privileged belligerent does not suffer any of these limitations. She can kill her victim while he sleeps from one thousand miles away, facing no imminent threat whatsoever.[42] For this privileged belligerent to gain this legal authority to target and do violence to others, however, she must first set herself out as a

---

[37] The specific language used denotes privileged belligerency as a 'right.' "Members of the armed forces…have a right to participate directly in hostilities." Additional Protocol I, Art. 43(2).

[38] ICRC Commentary on the Additional Protocol I 1453 (¶4789) "Those who belong to armed forces or armed groups may be attacked at any time."

[39] In Gregg v. Georgia, 428 U.S. 153 (1976) the United States Supreme Court overturned its decision of four years earlier in Furman v. Georgia, 408 U.S. 238 (1972), and held that capital punishment was a lawful use of force and not prohibited by the 8th Amendment to the U.S. Constitution.

[40] Model Penal Code [MPC] §3.04 "…the use of force upon or toward another person is justifiable when the actor believes that such force is immediately necessary for the purpose of protecting himself against the use of unlawful force by such other person." & 3.05 "…the use of force upon or toward the person of another is justifiable to protect a third person when…the actor would be justified under Section 3.04 in using such force to protect himself."

[41] Tennessee v. Garner, 471 U.S. 1, 2 (1985).

[42] Tugendhat & Croft*, supra* note 26.

lawful target,[43] such that she can also legally be killed while sleeping by an enemy she has never met, let alone threatened. Combatants that distinguish themselves from civilians are the only individuals authorized to commit these violent acts of war authorized by *jus in bello*;[44] all others must comply with the mandates of criminal law.

(ii) The Responsibility to Target only Enemy Combatants and Military Objectives.

Though it may seem counterintuitive, the restriction to limit attacks to enemy combatants and military objectives applies only to combatants – privileged belligerents. This does not mean civilians – noncombatants – can target other civilians at will. It means if they are not a combatant, a civilian cannot target anyone, except when their conduct would be justified by traditional criminal law. Only the privileged belligerent can step outside the constraints of traditional criminal law, but when they do so, they must limit the targets of their attacks to enemy combatants and military objectives.[45]

B. The Principle of Military Necessity[46]

In addition to the principle of distinction, the concept of privileged belligerency is inextricably linked to a second principle of *jus in bello*, military necessity. Distinction clarifies what one must do to qualify for the privilege, and military necessity identifies what violent powers one is granted. In simplest terms, the principle of military necessity authorizes the combatant to do acts of violence against the enemy military that are needed to bring about the complete submission of that enemy and an end to the war.[47] Once again,

---

[43] Convention (III) relative to the Treatment of Prisoners of War. Geneva, 12 August 1949 [*hereinafter* "Geneva III"] at Art. 4.

[44] DOD LAW OF WAR MANUAL, paragraph 5.5.8.

[45] It is this second part of the Principle of Distinction that prohibits indiscriminate attacks. Thus, it is often referred to as the Principle of Discrimination. The authors view this as a subset of Distinction rather than a separate Principle.

[46] *See* DOD LAW OF WAR MANUAL*, supra* note 25.

[47] *Id.*

however, this does not apply to civilians or civilian law enforcement. Officer Groubert may have the mission to apprehend a violent felon, but without probable cause of a significant threat to the officer or others, he is authorized to only use ordinary force to make an arrest.[48] The principle of military necessity has both a permissive and a restrictive aspect, as well as providing the lawful combatant a moral foundation for his acts of violence.

1. *The Privilege of Strategic Justification for Acts of Violence.*

A civilian is authorized to do limited violence to rebuff an imminent threat. A civilian must justify each act of violence based on contemporaneous and proximate danger to themselves or others.[49] For the combatant, eliminating a threat to themselves is merely ancillary to their duty to win the war as rapidly as possible. Therefore, a combatant's acts must be evaluated in the much broader context of how they affect the war effort and not just the narrow frame of time and place the act occurred. A combatant can blow up a bridge built by farmers to get to their fields, not because of any threat posed by those farmers, but because she has reason to believe the enemy plans to use the bridge to transport troops across the river two weeks in the future.

2. *The Restrictive Side of Military Necessity.*

This principle is both permissive, allowing the combatant to do all acts necessary to win the war, and restrictive, prohibiting violent acts which would otherwise be lawful, if they are not needed for victory. On the restrictive side is the prohibition against attacks that cause unnecessary suffering.[50] Putting glass shrapnel in a grenade so subsequent surgery will be more difficult is an example of violence

[48] *See generally Gregg, 428 U.S.* (This is the rule of Tennessee v. Garner, 471 U.S. 1 (1985)).

[49] MPC §3.04 & 3.05.

[50] ICRC, Customary International Humanitarian Law, Rule 70.

that goes beyond the principle of necessity.[51] A second part of the restrictive side of military necessity (as well as the discrimination aspect of distinction) is the concept of humane treatment.[52] Once Soldiers become *hors de combat* by being injured, surrendering, or evacuating a sinking boat or crashing plane, they are no longer lawful targets. Further, the capturing party has a plethora of responsibilities for their welfare.[53]

3. *The Combatant's Raison d'Etre.*

Perhaps the most important aspect of military necessity is that it is inextricably linked to bringing about an end to hostilities. The lawful combatant is not a mercenary performing a service for a fee. Instead, she is the designated agent of the State sent to engage in and be the target of horrific violence. The lawful combatant loses the protections of the law and in exchange is offered immunity for their acts of combat. The moral individual would never stomach this loss merely so they can do greater acts of violence against strangers. They sacrifice, sometimes involuntarily,[54] the protections of the law for the higher purpose of bringing about an end to the armed conflict through victory over the enemy. The principle of military necessity protects their ability to achieve victory and thus provides the foundational explanation for the very existence of the military.

---

[51] Unnecessary Suffering is often cited as a separate Principle of *jus in bello*, but since it is merely the negative corollary of Military Necessity (One can do only that violence which is necessary, so causing suffering that is not is prohibited) we prefer to view it as a subset.

[52] Humanity or Humane Treatment is also often viewed as a totally separate Principle, but the authors view it as a subset of both Military Necessity and Distinction since its fundamental principles are again a limitation on unnecessary violence against noncombatants and the suffering thereof.

[53] Geneva III, *supra* note 43.

[54] The Selective Service Act, 50 U.S.C. §§ 201-214 (1917) required registration for a draft, or the governmental act of forcing an individual into the military.

C. The Principle of Proportionality

The principle of proportionality requires the anticipated result of any attack to bring about a military advantage exceeding the collateral damage to civilians and civilian property.[55] Like military necessity, this principle is both permissive and restrictive.

As noted above, the lawful purpose of a combatant's acts of war is *not* to secure their personal safety, but to bring about the end of the conflict. The latter is much more difficult to achieve as well as significantly more important to the international community. As such, the combatants have been granted far greater leniency than civilians when the effects of their violent acts are legally analyzed. If a civilian knowingly brings about the death of a non-aggressing person, this is considered intentional homicide even if the actor did not desire death to occur.[56] If Officer Groubert, while chasing a group of fleeing violent felons, knowingly drives his vehicle over and kills a bystander civilian to avoid losing his targets, this is murder regardless of his benevolent motive to stop the violent felons from escaping.[57] However, if a combatant blows up the enemy commander's car, purposefully killing him and knowingly killing his three-year-old daughter who is riding with him, the attack would be perfectly legal under *jus in bello* if the concrete military advantage gained by the commander's death outweighed the death of the innocent girl. As noted in the discussion of the principle of distinction, above, the combatant could never target the little girl, but under the principle of proportionality, her collateral death could be legally acceptable under *jus in bello*. Like military necessity, this concept of legally acceptable collateral damage is limited to the privileged belligerent. The civilian is not authorized to attack the enemy commander even if the girl is not present.

---

55 Additional Protocol I, art. 52.

56 MPC §210.2.

57 *Id.*

1. *The Goals of the Just War Theory.*

The two sides of the Just War Theory, *jus ad bellum* and *jus in bello,* have significantly different, though sequential and convergent goals. Both strive to limit the costs of armed conflict. The former attempts to achieve this by the singular goal of preventing the occurrence and existence of armed conflict. If *jus ad bellum* fails and armed conflict begins, it falls to *jus in bello* to limit the violence through three goals: ending the conflict, limiting the cost to lawful combatants, and limiting the violence done to noncombatants.

The goal of *jus ad bellum* is overt – to maintain international peace and security by preventing armed conflict.[58] This parallels the civilian government's law enforcement mission of maintaining peace and security by preventing violent (and nonviolent) crime.

The goals of *jus in bello*, though less obvious, can be gleaned from the three core principles discussed above. When viewed together, the requirement to distinguish oneself under the principle of distinction, the ability to do violence strategically motivated under military necessity, and the increased lenience towards collateral damage encapsulated within proportionality, coalesce into the purpose of bringing about a rapid end to the armed conflict. The concepts of privileged belligerency and humane treatment combine to evince a second purpose – limiting the cost of war paid by its participants. A third purpose, shown by the requirement of discrimination, is to limit the cost of war paid by the innocent civilian.

Each of these is a noble and laudable purpose integral to the Just War Theory. However, it appears that in the modern asymmetric environment, some want to prioritize the third goal to the detriment of the first two. Comments and decisions by leaders, academics, and jurists who desire to prevent military violence, while laudable, reflect a lack of appreciation of the first two purposes in the *jus in bello* paradigm as well as the core legal concepts within this *lex specialis*.

[58] Preamble to the UN Charter.

2. *The Required Gap Between Civilians and Privileged Belligerents Under the Lex Specialis of Jus in bello.*

The foundation of all *jus in bello* is the concept of privileged belligerency. The legal gap between the privileged belligerent and the civilian is arguably greater than any other that could be drawn between two people. While the police officer may have more legal authority to use some force than the citizen, it pales in relation to the Soldier's license to kill. The death-row convict may have forfeited his fundamental right to life based on his prior acts, but he still stands closer to the ordinary citizen than the Soldier whose life becomes legally forfeit through no act of his own.[59] This gap is why the first and most important question of evaluating the legality of *any* act of combat is: was the actor a privileged belligerent?

If the answer to this antecedent question is no, there is no need to look to the *lex specialis* of IHL to evaluate their conduct; criminal law is fully capable of this adjudication. However, if the answer is yes, the actor was a privileged belligerent, then criminal law is irrelevant and *only* IHL should be used to evaluate their acts of combat.[60]

If a person is unprivileged (*i.e.*, a civilian), he is prohibited from the use of violence against persons or property of another except when that conduct is legally justified or excused and a proportional response to an imminent threat. This prohibition is the product of the comparatively consistent jurisprudence of criminal law developed over millennia. In contrast, the privileged belligerent *(i.e.,* the Soldier) is permitted to use violence to destroy property and kill people. Further, these acts of violence can be grossly disproportional to a threat that is distant in both time and place. For example, a privileged belligerent controlling a piece of field artillery in an armed conflict can use the weapon to kill 1,000 enemy Soldiers 20 miles

[59] As stated above, even involuntary membership in the armed forces makes you a lawful target of the enemy privileged belligerent.

[60] The legal maxim is *"lex specialis derogat legi generali"* so the *lex specialis* of IHL takes precedence over the more general criminal law.

away even if they are sitting down to dinner and have no plans to attack him.[61]

For the civilian, the battlefield, in and of itself, does not grant him any additional legal authority to use force. Legally, a citizen on the battlefield operates under the same restrictions as one caught in a gunfight between police and a group of bank robbers. The situation may give rise to the legal ability to use violence based on justification (self-defense) or excuse (necessity), but this will be factually dependent and temporarily linked to the existence of a given imminent threat.[62]

The Soldier goes through a dramatic legal conversion once armed conflict begins. The Soldier morphs from a civilian legally indistinguishable from any other concerning the use of force, to a new type of legal entity authorized by the world community to use deadly force. As noted above, the Soldier is even authorized to knowingly kill innocent civilians, provided their deaths are outweighed by the concrete military advantage gained.

Criminal law prohibits a civilian from using force or violence except in narrow circumstances such as self-defense. Therefore, the principles embedded in *jus in bello* – military necessity, proportionality, and distinction – do not provide any additional legal guidance with which to evaluate their acts. A civilian is not allowed to use violence to achieve his goals, military or otherwise, so the principle of military necessity never applies. A civilian is prohibited from knowingly or recklessly causing the deaths of innocent civilians, or damage to their property, so any argument that the loss was proportional to what he hoped to gain will fall on deaf ears. Concerning distinction, a civilian is not authorized to use unjustified violence against any target,

---

[61] The concept of proportionality limit collateral damage to civilians and civilian property, it does not limit damage to lawful targets. Members of the enemy military are lawful targets at all times unless they become *hors d'combat* by surrendering, being wounded to the point they can no longer fight, becoming unconscious, entering the water after their warship is sunk, or parachuting from a destroyed aircraft for safety.

[62] MPC §3.

whether it be military or civilian, so limiting his strikes to military targets is legally insignificant.[63]

A Soldier can be killed on the battlefield, but she is immune from prosecution or punishment for her lawful acts of combat, (*i.e.*, as long as her battlefield acts do not violate *jus in bello* she cannot be criminally judged even if her side loses the war). The rationale is Soldiers have no control over if or when they will be sent to armed conflict; therefore, it is patently unjust both to punish them for that collective decision (*jus ad bellum*) and to use rules which are applicable domestically (criminal law instead of *jus in bello*).

III. PART II – CONFLATION & MISUNDERSTANDING ERRORS IN THE TREND AGAINST THE USE OF MILITARY FORCE

The errors in the trend against the use of military force fall into five general categories: 1) a conflation of *jus in bello* with *jus ad bellum*; 2) a morphing of the military mission away from traditional war-fighting responsibilities, thereby frustrating the *jus in bello* goals of a rapid end to the conflict and limiting the cost to the warfighter; 3) a conflation of *jus in bello* concepts with similar terms in the traditional criminal law paradigm; 4) an attempt by some academics to revise time-tested principles in IHL that are the product of centuries of customary practice, and, 5) a general lack of military deference in modern courts by jurists with no military experience or valid frame of reference.

The costs of these errors are high: an ineffective military prolongs armed conflict through impotence and indecision, and victimizes the modern warfighter by leaving her outside the protections of the law; denying her the higher purpose of ending the armed conflict; and, reducing her to the legal peer of the criminals[64] she is forced to oppose.

---

[63] *Id.*

[64] This refers to the enemy combatants that disregard the principles of *jus in bello* by failing to distinguish themselves by wearing a uniform and carrying arms openly, among other violations. They can be labeled as criminals because they do

A. Trend 1: the *Jus ad bellum*'s Veneer Over *Jus ad bello*

As already outlined and discussed throughout this article, *jus ad bellum* and *jus in bello* are separable concepts. The public is comfortable and familiar with evaluating the merits of a given side in an armed conflict; it is a regular part of the political discourse and the fundamentals of *jus ad bellum* are similar to the restrictions on the use of force they face in everyday life. Public discourse is a good thing and the decision to enter an armed conflict should be widely and publicly debated. However, politicians, commentators, jurists, and academics then allow this *jus ad bellum* decision to enter an armed conflict to color and affect how they discuss and evaluate the legality of the combatant's acts in *jus in bello*. The conflation of *jus ad bellum* and *jus in bello* is both legally and morally problematic.[65] The two concepts are distinct but can become blurred when the reasons behind why a State entered an armed conflict are suspect or without merit.

World War II is a perfect example to compare one State's Soldier with another: the German Soldier and his American counterpart. The German Soldier was a product of an evil State. But the rules governing the German Soldier in combat are identical to the rules that govern the U.S. Soldier in combat. The validity of a *jus ad bellum* claim that a war is unjust is totally irrelevant to the legality of a given warlike act of a Soldier. As the Just War Theorist Professor Michael Walzer notes, just wars can be fought unjustly and unjust

---

not possess privileged belligerency and therefore all of their acts of violence, to include the killing of uniformed enemy, are subject to criminal prosecution.

[65] This issue has been identified in the DOD LAW OF WAR MANUAL:

"As a general matter, *jus in bello* and *jus ad bellum* address different legal issues and should not be conflated. Conflating *jus in bello* and *jus ad bellum* risks misunderstanding and misapplying these concepts. For example, in *jus ad bellum*, proportionality refers to the principle that the overall goal of the State in resorting to war should not be outweighed by the harm that the war is expected to produce. However, proportionality in *jus in bello* generally refers to the standard that the expected incidental harm to the civilian population and civilian objects should not be disproportionate to the anticipated military advantage from an attack. Therefore, although a *jus ad bellum* proportionality analysis might consider the harm suffered by enemy military forces in the fighting, a *jus in bello* proportionality analysis would not." *Id.* at 3.5.1.

wars can be fought justly.[66] While politics are a necessary part of *jus ad bellum*,[67] we should be careful to keep politics from affecting any *jus in bello* legal determinations and adjudication just like we try to keep politics out of our domestic criminal law decisions.

This task is difficult enough without being linked to the modern international criminal tribunal whose jurists do not share a common polity with the defendant or even with each other. While these same conditions existed at Nuremberg, many of those judges were military officers fully aware that the decisions they made would affect their profession. Conversely, few judges at the international tribunals have any military experience.[68] This lack of military experience is evident in many of our politicians, commentators, jurists, and academics; the result is that they tend to be far more familiar with and accepting of the criminal law and *jus ad bellum* goals of maintaining the peace rather than the *jus in bello* mission of rapidly ending the war.

B. Trend 2: The Current Mindset for War: From the Management of Violence to the Management of Governance

The role of the modern military is changing and today's militaries face great uncertainty. New technologies and capabilities to inflict harm are not only held by States but are in the hands of non-State actors.[69] In *War From the Ground Up*, Emily Simpson divides modern conflict into two categories: war fought "to establish military

---

[66] WALZER *supra* note 29, at 21.

[67] For example, the Article 1, section 8 of the U.S. Constitution give the power to declare war to the most political of the three branches of the Federal Government: Congress.

[68] For a discussion of the cost of a lack of military experience among Tribunal judges, see Richard V. Meyer, *Following Historical Precedent: An Argument for the Continued Use of Military Professionals as Triers of Fact in Some Humanitarian Law Tribunals,* 7 J. OF INT'L CRIM. JUST. 43 (2009).

[69] A byproduct of the post-industrial information age is that the raw materials and the knowledge to manufacture or develop potent weapons are both readily available to the general populace.

conditions for a political solution;"[70] and war fought to "directly seek political, as opposed to military, outcomes."[71] The Gulf War from 1990 to 1991 is a modern example of the first type while Afghanistan is an example of the second. The reality of having a strategy that needs "to consider military actions in terms of their likely political interpretations"[72] will persist. As Simpson correctly notes, General Stanley McChrystal, the Commander of the International Security Assistance Force (ISAF) in Afghanistan in 2009, restricted the use of both indirect fires and air-delivered bombs not because "they are . . . effective in military terms; they are. However, their political effect is often more harmful than their military value."[73] McChrystal put it in more general terms in his tactical directive: "the carefully controlled and disciplined employment of force entails risk to our troops – and we must mitigate that risk wherever possible. But excessive use of force resulting in an alienated population will produce far greater risk."[74] The political and the military become blurred: "A policy decision only to fight wars with clear military solutions would mean to decline involvement in several situations in which enemies, especially non-state actors, refuse to engage in conventional battle against Western military forces."[75]

In 1957, Professor Samuel Huntington wrote *The* Soldier *and the State,* in which he outlined what constituted a professional Soldier.[76] Professor Huntington opined the Soldier's purpose was "the management of violence."[77] But the modern Soldier is asked to do much more. Today's Soldier is asked to manage governance: Soldiers build schools, teach judges, manage power plants, grow

---

[70] Sir Michael Howard, TIMES LITERARY SUPPLEMENT (Apr. 13, 2013) (reviewing ERNIE SIMPSON,' WAR FROM THE GROUND UP: TWENTY-FRIST-CENTURY COMBAT AS POLITICS (2013 [*hereinafter* "Simpson"]).

[71] *Id.*

[72] *Id.* at 4.

[73] *Id.* at 234.

[74] Declassified excerpt from NATO's Tactical Directive, 2 July 2009, released by NATO ISAF Headquarters, 6 July 2009.

[75] Howard, *supra* note 70, at 11

[76] SAMUEL HUNTINGTON, THE SOLDIER AND THE STATE (1957).

[77] *Id.* at 16.

crops.[78] Even in non-permissive environments, Soldiers are expected to mitigate violence. In concept, mitigating violence is attractive, but in practice, the asymmetric enemy is unlikely to give the Soldier any indication that he or she is a belligerent.

One example of this thinking is the U.S. Army and the U.S. Marine Corps manual for counterinsurgency (COIN).[79] Understanding the asymmetric reality of both Iraq and Afghanistan, the military decided in the mid-2000s to redraft the COIN manual. In particular, the situation in Iraq had deteriorated and the insurgency was gaining momentum. The manual, published in June 2006, acknowledged "[a]t its core, counterinsurgency warfare is a struggle for the support of the population. Their protection and welfare is the center of gravity for friendly fire."[80] One of the enumerated 'unsuccessful practices' in the counterinsurgency manual was the warning not to place a "priority on killing and capturing the enemy. . ."[81] The goal instead is to engage and protect the population.

Counterinsurgency is an example of the second form of warfare discussed by Simpson; Counterinsurgency's core mission is to make a political reality happen. This means political factors are primary. In the case of Afghanistan, it was the popular legitimacy of the government. In the words of Ambassador Karl Eikenberry, "[b]roadly stated, modern COIN doctrine stresses the need to protect civilian populations, eliminate insurgent leaders and infrastructure, and help establish a legitimate and accountable host-nation government able to deliver essential human services."[82]

The COIN doctrine allows the use of force, to include lethal force, but the entire narrative of the manual is to constrain the use of force:

---

[78] Dominic Tierney, Op-Ed., *Jefferson's Army of Nation Builders*, N.Y. TIMES, Nov. 10, 2010.

[79] Counterinsurgency, Field Manual 3-24/Marine Corps Warfighting Publication 3-33.5, December 2006 [*hereinafter* "COIN Manual"], at Preface.

[80] *Id.* at 1.1.

[81] *Id.*

[82] Karl W. Eikenberry, *The Limits of Counterinsurgency Doctrine in Afghanistan: The Other Side of the COIN*, FOREIGN AFFAIRS, Sept./Oct. 2013, at 59, 63.

> [a]ny use of force generates a series of reactions. . . .the type and amount of force to be applied, and who wields it, should be carefully calculated by a counterinsurgent for any operation. An operation that kills five insurgents is counterproductive if the collateral damage or the creation of blood feuds leads to the recruitment of fifty more.[83]

This rationale and logic was clear in the 2011 tactical directive of the Commander of ISAF, General John R. Allen, which stated:

> [c]onsider all use of force carefully. Ensure that the use of force is necessary and proportionate to the threat faced, and when applied it is precisely delivered. We must never forget the center of gravity in this campaign is the Afghan people; the citizens of Afghanistan will ultimately determine the future of their country.[84]

During the same time frame the COIN concept was being developed within the Department of Defense, the Office of the Chairman of the Joint Chiefs of Staff enacted a breathtaking change to the Standing Rules of Engagement (SROE): individual Soldiers no longer enjoyed the personal right of self-defense.[85] Individual self-defense became a subset of unit self-defense and exercised by the unit commander: "unit commanders may limit individual self-defense by members of their unit."[86] The theoretical foundation of individual self-defense is premised on three pillars: the force used is necessary; the amount of force used is proportional; and the threat is imminent. In the previous editions of the SROE, the U.S. recognized each

---

[83] COIN Manual, paragraph 1-141

[84] ISAF Tactical Directive, 30 November 2011, found at http://www.rs.nato.int/images/docs/20111105%20nuc%20tactical%20directive%20revision%204%20(releaseable%20version)%20r.pdf.

[85] Joint Chief's of Staff Instruction 3121.01B, Standing Rules of Engagement, 13 June 2005 at para. E.2.a.

[86] *Id.*

Soldier possessed the "inherent right to use all necessary means available and to take appropriate actions to defend oneself. . . ." [87]

The suspension of an individual Soldier's right of self-defense and the ascent of the COIN doctrine are inextricably related; the concept of limiting the use of force is woven throughout the counterinsurgency manual.[88] The suspension and ascent are related by time, effect, and circumstances on the ground in both Afghanistan and Iraq in 2004 and 2005. There was a conclusion that military commanders could not use violence to win the conflict. And the COIN doctrine, by its very nature, and the suspension of self-defense, limits the use of force.

The COIN doctrine during an insurgency is not ill-advised; this doctrine is a legitimate means to execute a war. But the desire to limit force has a profound effect on a State's military. The management of violence by the Soldier under COIN is the exception; now, under Simpson's second paradigm, the Soldier is focused on managing governance. The military activity is no longer clearly distinguishable from the political activity by the Soldier on behalf of State. This means we enter a conflict where military violence is eschewed. Conditions allowing the use of force to be confined and constrained is, however, a policy decision. Counterinsurgency policy does not change the law that applies to combatants in conflict. It does, however, change the public's mindset of what war constitutes. The public begins to think we can produce results with limited force. It then becomes the expectation – especially from the public, via the press – that any force which results in a death of an innocent is the exception. It drives the public to believe the resultant damage or death is the salient factor in considering if a force was justified to begin with.

In other words, civilian criminal law standards start to apply to privileged belligerents on the battlefield. Terms like self-defense, necessity, and proportionality exist both within criminal law and *jus in bello*. This leads some to think the *jus in bello* standards imbedded in

---

[87] Joint Chief's of Staff Instruction 3121.01A, Standing Rules of Engagement, 15 January 2000 at Enclosure A, para. 5.a.

[88] COIN Manual, *supra* note 79.

IHL are the same language: the same concepts and meaning extrapolated from civilian criminal law. The media, commentators, and even jurists are guilty of this mistake. The fact is, although the vocabulary may be similar, the meaning of these terms is tectonically different. This category of conflation error has recently arisen within the decisions of the international tribunals.

C. Trend 3: Criminalization of the Use of Force by International Courts

Military objectives are central to the use of violence by a military commander. Military objectives are "limited to those objects which by their nature, location, purpose or use 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."[89] The sad reality is that civilians, who are protected by IHL, will inevitably be in areas of armed conflict and exposed to harm. It is therefore universally recognized, in the words of Professor Geoffrey Corn, "that the principle of military objective is insufficient to provide adequate protection for civilians from the harmful effects of hostilities."[90] With this reality in mind, military professionals, through customary practice, developed the *jus in bello* principles of distinction and proportionality. These were recorded by the drafters of the Geneva Conventions Additional Protocol, which prohibits 1) attacks that are intentionally against civilians and 2) attacks that produce excessive civilian casualties in relation to the concrete military objective.[91]

The first prohibition is intent based; the second is a balancing of military objectives and the civilian casualties and determining if the latter was excessive. The first violates the principle of distinction, while the second violates the principle of proportionality. Distinction, as noted earlier, is the obligation of military personnel to delineate

---

[89] Additional Protocol I, 52(2).

[90] Expert Report of Professor Geoffrey Corn to the ICTY for the case of The Prosecutor v. Ante Gotovina, Ivan Cermak and Mladen Markac, IT-06-90, at 12.

[91] Additional Protocol I, 48 & 51(5)(b).

between combatants and civilians. Proportionality is a much more ambiguous concept because it is subjective; proportionality is violated, in essence, when it is determined that the harm to civilians was excessive to the concrete and direct military advantage anticipated from attacking a lawful military objective. Professor Jens David Ohlin of Cornell University concludes, "that there are almost no examples of [proportionality-based] prosecutions before international tribunals that might provide guiding precedent on the nature of proportionality."[92] Professor Ohlin maintains that proportionality "has so rarely been applied by international tribunals" because prosecutors "squeeze almost all of the targeting cases into the first [prong], thus accusing the commander in question of directly targeting civilians. . . ."[93]

Outlining a series of cases with the International Tribunal of the Former Yugoslavia (ICTY), Professor Ohlin concludes the common law concept of intent—acting with purpose or knowledge—required under the first prong of intentionally attacking civilians within the ICTY has morphed to the lower standard of recklessness. In other words, the court never has to grapple with the murky world of proportionality found in the second prong. The case that crystallizes this lower standard is *The Prosecutor v. Pavle Strugar.*[94]

In *Strugar*, the defendant, Lieutenant General Strugar, was a leader in the then Yugoslav Peoples' Army.[95] The Yugoslav government, in an attempt to hold Yugoslavia together, was attempting to suppress the Croatian people from breaking away.[96] As part of this suppression, General Strugar shelled areas of Dubrovnik, Croatia in late 1991.[97] These artillery attacks killed several civilians

---

[92] Jens David Ohlin, *Targeting and the Concept of Intent*, 35 MICH. J. INT'L L. 79 at 86 [*hereinafter* "Ohlin"].

[93] *Id.*

[94] *Id.* citing Prosecutor v. Strugar, Case No. IT-01-42-T, Trial Chamber Judgment, Int'l Crim. Trib. for the Former Yugoslavia (Jan. 31, 2005), http://www.icty.org/x/cases/strugar/tjug/en/str-tj050131e.pdf. [*hereinafter* "Strugar"].

[95] *Id.* at 1.

[96] *Id.*

[97] *Id.*

and destroyed many historic buildings.[98] The defendant was charged with murder and the intentional attacks on civilians. He was found guilty and sentenced to eight years.[99] The Trial Chamber held:

> . . . where a civilian population is subject to an attack such as an artillery attack, which results in civilian deaths, such deaths may appropriately be characterized as murder, when the perpetrators *had knowledge of the probability* that the attack would cause death.[100]

The mere probability the attack would cause death is enough to trigger a charge of an intentional harming of civilians. The concept of intent—acting with either purpose or knowledge—under *Strugar* expanded to recklessness. This lower standard means a commander who launches an attack where there is a probability civilians might be injured or killed is violating IHL; in other words, the commander launching the attack is a war criminal because of mere probability and the accompanying result that the harm occurred. In war, it would be hard to fathom a situation where harm might not befall the civilian population, especially in an age of asymmetric warfare where the enemy refuses to distinguish himself from the civilian population.

What is occurring is that the law is being driven by the results, not the intent. War causes death and destruction and some of those harmed will be civilians. To minimize those losses is of paramount import, but to make the standard of culpability one of recklessness subject to an after-the-fact review is to impose an unrealistic limitation on the military. And conceptually, it flips IHL on its head. Professor Ohlin states the conceptual underpinnings of IHL: "envisioning the killing of civilians and coming to some conclusion as to whether the number of deaths will be proportionate or not disproportionate – does not violate the principle of distinction. Simply envisioning the deaths of civilians does not mean the commander has directed the attack against the civilians."[101] If that

---

98 *Id.*

99 *Id.* at 198.

100 *Id.* at 110.

101 Ohlin, *supra* note 92, at 113.

were the case, no Soldier would be immune from the reality that in war civilians will be killed and thereby making Soldiers criminally liable to this reality.

Even the mental element in Article 30 of the Rome Statute of 1998—the Statute that established the International Criminal Court (ICC)—states "[u]nless otherwise provided, a person shall be criminally responsible and liable for punishment for a crime within the jurisdiction of the Court [ICC] only in the material elements are committed with intent and knowledge."[102] A plain reading of Article 30 seems to suggest the defendant must act with purpose or knowledge to be culpable. In fact, recklessness as a standard to meet culpability was considered by the drafters of the Rome Statute and squarely rejected: the mental element of recklessness was banished from the Statute.[103] Put differently, even if an accused foresees the *possibility* of his or her act causing death and still persists, regardless of the possible consequences, the person is *not* guilty of a war crime unless the accused had knowledge civilians would be killed and he or she meant to kill those civilians.

But some judges and commentators cite Article 30 and the "unless otherwise provided" clause to conclude recklessness is enough to find culpability. Recklessness, they argue, is a level of intent that is an acceptable standard under customary international law and therefore, otherwise provided; that is, it is an acceptable mental state for war crimes.[104] Professor Ohlin notes, however, "it is not clear how customary international law could provide a basis to support a lower mental element."[105] This revisionist interpretation of what Article 30 means is critical because it changes the focus from what the Soldier thinks *will* happen to what an objective person thinks *might* happen. Those are two starkly different perspectives. The former is a mental state possessed by the Soldier when he uses force, while the latter is about the degree of risk the Soldier takes. Any military mission will have risks that the Soldier's acts could cause the

---

[102] Rome Statute of the International Criminal Court, (entered into force July 1, 2002) at Article 30 [*hereinafter* "Rome Statute"].

[103] *Id.*; Ohlin *supra* note 92, at 101.

[104] Strugar, *supra* note 94, at 110.

[105] Ohlin, *supra* note 92, at 108.

death of a civilian – if that is the acid test, however, then any mission will be judged under the first prong of willfully targeting civilians. Under this analysis, the courts approach a strict liability: the dead civilian is presumptively a war crime.

The courts' decisions and even the far better justified opinion of Professor Ohlin both make the same conflation error; attempting to use traditional criminal law concepts to explain terms in *jus in bello*. Professor Ohlin falls for the trap of using the common law definition of intentional (including purpose and knowledge) to define the term within the Protocol and opening this door invites the subsequent step down to recklessness. This first prong actually has two parts: A) who or what was targeted, and B) were they or it a legitimate military target?

Part A is entirely subjective. Who were you targeting? Combatants are prohibited from conducting indiscriminate attacks. Instead, each attack must have a specific legitimate military target. Thus, for the first prong, the standard is that of motivated purpose. As the then Chief Prosecutor of the International Criminal Court noted, "International humanitarian law and the Rome Statute permit belligerents to carry out proportionate attacks against military objectives even when it is known that some civilian deaths or injuries will occur."[106] To use any other standard would be to completely eliminate the principle of proportionality. That principle forces the attacker to balance the military advantage with the collateral damage, meaning the attacker has knowledge a civilian target will be damaged and yet can still strike if the military advantage outweighs the collateral cost. The crux is who or what did they plan for the projectile to hit?

For part B, if the target was a valid military target, this part has not been violated even if the strike (knowingly) killed dozens of innocent civilians collaterally, though this would probably violate the second prong of proportionality. More problematic is if the shooter

[106] Luis Moreno-Ocampo, letter concerning the situation in Iraq, Office of the Prosecutor, International Criminal Court, February 9, 2006, p. 5, available at http://www.iccnow.org/documents/OTP_letter_to_senders_re_Iraq_9_February_2006.pdf.

subjectively believed the target to be a valid military target, but in fact it was not. For example, Captain Kudo shot the two diggers on the side of the road in Afghanistan believing they were planting a bomb, but afterwards we determine they were only digging an irrigation canal. It is in this second prong that a level of intent less than purpose might be appropriate. On a static battlefield (*e.g.*, trench warfare) segregated from the civilian population, it might be justifiable to issue an order to shoot anything moving in the no man's land between the trenches since there is little or no chance it is a civilian and taking the time to verify it is an enemy may place the Soldier at risk. This would be in contrast to a modern asymmetric nonlinear global battlefield. Given these opposite poles of possibility and correlative responsibility, the sliding scales of recklessness or negligence seem to provide the best vehicle to balance the myriad of factors and concerns. However, post hoc evaluation of any such decision must give full credence to the factual situation for that belligerent: would a reasonable privileged belligerent with the knowledge, training, time, resources, and experience of the defendant have *believed* the target was lawful? Note this does not open the door to question if the attack was tactically required at that time under this prong, but only if the belief of the shooter that the target was a military target was reasonable under the circumstances.

On at least one occasion, the ICTY grappled with the second prong: attacks that produce excessive civilian casualties in relation to the concrete military objective. In the case of *The Prosecutor v. Ante Gotovina, et al.*[107], Colonel General Ante Gotovina, a Croatian commander, was indicted for ordering an illegal artillery attack against four towns—Knin, Obrovac, Gracic and Benkovac.[108] Each city was in the Croatian Serb break-away region of Krajina. Croatia launched an offensive—Operation Storm—in 1995 to bring this region back under Croatian control. The Croatian forces commenced to put the towns of Knin, Obrovac, Gracic and Benkovac under fire.[109] The objective of Operation Storm was to expel Serbian forces from the region. The Croatian forces succeeded under General

[107] The Prosecutor v. Ante Gotovina, Ivan Cermak and Mladen Markac, IT-06-90 [*hereinafter* "Gotovina"].

[108] *Id.* at 9.

[109] *Id.* at 601.

Gotovina; they seized Knin, the capital of Krajina, on August 5, 1995.[110]

The Tribunal's indictment of General Gotovina for violations of the laws and customs of war hinged on his shelling of the four towns. The Trial Chamber found General Gotovina guilty of violating these laws and customs. As one academic concluded, "Gotovina's conviction turns on the lawfulness vel non of the artillery fires against targets in the[se] Krajina towns. . . ."[111]

The Trial Court's judgment of Gotovina appears to be premised on both prongs of liability: the attacks were intentional (i.e., deliberately toward civilians), and the attacks were indiscriminate (i.e., an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated).[112] As Major General Walter B. Huffman, the former Judge Advocate General of the U.S. Army, noted, "the court apparently embraced a hybrid theory of both deliberate and indiscriminate targeting in violation of Protocol I, Articles 51(2) and 51(5)(a).[113] Under Article 51(2), the first prong—"civilians [] shall not be the object of attack"—Gotovina "deliberately targeted civilian areas."[114] Under Article 51(5), the second prong—the balancing of the military advantage gained to the amount and severity of civilian casualties —Gotovina's shelling "constituted an indiscriminate attack on these towns. . ."[115]

Both prongs are premised on an inference that shells that landed more than 200 meters from a known military objective were deemed unlawful (deliberate or indiscriminate) attacks on civilian

---

110 *Id.*

111 Walter B. Huffman, *Margin of Error: Potential Pitfalls of the Ruling in the Prosecutor v. Ante Gotovina*, 211 MIL. L. REV. 1, 13 (2012) [*hereinafter* "Huffman"].

112 ICRC, Customary International Humanitarian Law, Rule 12; Additional Protocol I, Art. 51(5)(b).

113 Huffman, *supra* note 111, at 28.

114 Gotovina, *supra* note 107, at 973

115 Huffman, *supra* note 111, at 28.

areas.[116] With little evidentiary support, the Trial Chamber concluded "a reasonable interpretation of the evidence that those artillery projectiles which impacted within a distance of 200 meters of identified artillery targets were deliberately fired at that artillery target."[117] The court then extrapolated from this norm that any projectile falling outside the 200-meter range was disproportionate.[118]

The Trial Chamber's decree of a 200-meter rule—without receiving any evidence on this point—is deeply troubling: "the court had to make broad assumptions, treat the absence of evidence as evidence of absence, and resolve ambiguities in favor of the prosecution to be able to apply its 200 meter standard."[119] The logic in the *Gotovina* case extends the trend outlined by Professor Olin that the threshold of liability is lowered, but in this case, it goes to the second prong. International Tribunals' attempt to shoehorn all civilian deaths into an intentional act, even if reckless, under the first prong (the military commander knew there would be civilians casualties), is driven by the prosecutor's theory of the case. Opening the aperture to recklessness is concerning and fraught with dangers. In essence, the court's focus is on the post-hoc effects of the military's attack instead of what is required by IHL; that commanders act in good faith to do all within their capabilities and limitations to minimize civilian casualties while accomplishing their mission.[120] The *Gotovina* Court, however, introduces a *per se* rule into the subjectivity of proportionality. The court dictates that since the commander exceeded the 200-meter rule, he is *per se* excessive under the second prong.

When triggering a *per se* rule, an international tribunal never has to contend with the commander's intent and examine his good-faith precautions to spare innocence. Like reducing intentionality to mere recklessness, the court sidestepped the rigorous balancing

---

[116] Gotovina, *supra* note 107 (Summary at http://www.icty.org/x/cases/gotovina/tjug/en/110415_summary.pdf).

[117] *Id.*

[118] *Id.*

[119] Huffman, *supra* note 111, at 36.

[120] ICRC Commentary on International Humanitarian Law, note 22 at para. 2215.

analysis required under the principle of proportionality. Instead, the *Gotovina* Court relied on a strict liability of violating some abstract rule of distance to find liability. To abandon this balancing test is problematic to say the least.

As General Huffman concludes, "[a] hallmark of international humanitarian law is its consistency with the actual practice of warfare by civilized nations."[121] The court's per se 200-meter rule, made out of whole cloth, alters the timeframe to be examined; in other words, the moment in time for consideration is shifted from the time of attack to the time the collateral damage occurs. This is contrary to IHL in that the question of whether the commander killed or injured civilians becomes the locus of judgment instead of examining the commander's military necessity at the time of attack. Even the commentary to the Additional Protocols acknowledges that under the second prong, when determining if the harm to civilians is excessive to the concrete and direct military advantage anticipated from an attack of a lawful military objective, the perspective to be examined is the military commander's before the attack.[122] It is the prosecution's obligation under the customs and laws of war to show there was a criminal intent by the commander when he ordered the attack. The destructive results are evidence but nothing in the law requires, nor should it, the results be the driver. It is the commander's intent at the time.

The Appeals Chamber reversed the Trial Chamber's conviction and found the 200-meter rule to be arbitrary; it further concluded the civilian casualties were not excessive compared to the military advantage from shelling the four towns.[123] As one military and artillery expert opined, "I can state unequivocally that a circle of 200 m[eters] around a target could never serve as a realistic or proper

---

[121] Huffman, *supra* note 111, at 45.

[122] Commentary to the Additional Protocols to the Geneva Conventions at pp. 683,684.

[123] Prosecutor v. Gotovina et al., Case No. IT-06-90-A, Appeals Chamber Judgment, (Int'l Crim. Trib. for the Former Yugoslavia (Nov.. 16, 2012) at http://www.icty.org/x/cases/gotovina/acjug/en/121116_judgement.pdf at pp. 19-21.

standard for a sound assessment of cannon and rocket fire. . . ."[124] Although set aside, the *Gotovina* Trial Court opened the door for international tribunals to stitch new rules out of whole cloth that impose criminal liability on commanders. As General Gotovina's appeal correctly asserts the judgment "has far-reaching significance beyond [his] case. . . . The Judgment is an unreasonable and unrealistic precedent that undermines that credibility and relevance of [international] humanitarian law. It imposes a standard so exacting that it renders lawful warfare impossible for military commanders."[125]

Professor Corn submitted an expert report before the trial court and in subsequent writings opined that the Tribunal was left with differing opinions on the reasonableness of General Gotovina's judgment.[126] Professor Corn's concern is that the International Tribunal seemed to base its reasonableness of Gotovina's actions on an assessment of whether a commander considered evidence in support of his decision.[127] But this should not be the standard in a criminal proceeding for reasonableness. Instead, the gravamen of the proceedings should be "on the quality of the evidence that supported the [commander's] decision."[128] In a nutshell, Professor Corn makes the point that, "[i]nstead of focusing on the question of whether the commander reasonably believed the object of attack was a military objective, the Tribunal has focused on the question of whether the commander knew the object of attack was a civilian or civilian property."[129]

The reality is that any criminal judgment of a Soldier using force will be after the fact—post hoc. The test must be one of

---

[124] Huffman citing Comments and Conclusions by GenMaj (ret.) Rolf Th. Ocken, German Army, on the Subject "Croatian Army use of Artillery in KNIN, CROATIA on 4-5 August 1995," (Nov. 19, 2011).

[125] Notice of Appeal of Ante Gotovina, Case No. IT-06-90-A, May 16, 2011, found at http://www.icty.org/x/cases/gotovina/custom6/en/110516.pdf at pp 4-5.

[126] Geoffrey S. Corn, *Targeting, Command Judgement, and a Proposed Quantum of Information Component: A Fourth Amendment Lesson in Contextual Reasonableness*, 77 Brook. L. Rev. 437, 456-457.

[127] *Id.* at 458.

[128] *Id.*

[129] *Id.*

reasonableness, but the analysis should start with what information did the commander have at the time? Professor Corn was "struck by the inherent arbitrariness of [the court's] assessment."[130] Professor Corn writes, "[w]hile it seemed relatively apparent that the Presiding Judge was determined to critique the reasonableness of General Gotovina's judgments by carefully considering all the facts and circumstances prevailing at the time, there was never any discussion of the amount of proof required to render those judgments reasonable."[131]

This lack of standard will inevitably drive a judicial appraisal to make determinations on what occurred after the fact vice the considerations and deliberations of the Soldier before the fact. The real question is: do the military actions have a reasonable basis in military necessity? The presumption must be yes. To presume otherwise would lead to the post hoc critiquing of a commander's actions based on what occurred, instead of the commander's intent as expressed by his orders.

D. Trend 4: Revising *Jus in bello* Without Considering the Effect on the Innocent Warfighter

Jus in bello is the evolved product of centuries of customary practice. Professional warfighters with battlefield experience have balanced humanitarian goals with the moral and legal mandate to end the conflict as quickly as possible and the rights and respect owed the individual warfighter to create the principles of *jus in bello*. By developing through customary practice, these principles were able to evolve without threatening the military mission or unjustly victimizing the warfighter. The battlefield is so dissimilar to everyday life because its denizens operate outside the protections of the law. The battlefield is not the place for external academic, untested, new-idea-driven change. Sadly, this has not dissuaded some from attempting exactly that.

---

130 *Id.* at 457.

131 *Id.*

In 2009, the International Committee of the Red Cross (ICRC) sent a shock wave across the international legal community. The ICRC published its Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law. In this Interpretive Guidance, written by Nils Melzer, the following recommendation was proposed:

> Restraint on the use of force in direct attack
>
> In addition to the restraints imposed by international humanitarian law on specific means and methods of warfare, and without prejudice to further restrictions that may arise under other applicable branches of international law, the kind and degree of force which is permissible against persons not entitled to protection against direct attack must not exceed what is actually necessary to accomplish a legitimate military purpose in the prevailing circumstances.[132]

It was the phrase "must not exceed what is actually necessary"[133] that caused the firestorm. The ICRC recommended a use-of-force continuum theory, or as some academics refer to it, the 'least harmful means rule.' In the Interpretive Guidance, the ICRC goes on to explain what it meant by necessary:

> [i]n sum, while operating forces can hardly be required to take additional risks for themselves or the civilian population in order to capture an armed adversary alive, it would defy basic notions of humanity to kill an adversary or to refrain from giving him or her an opportunity to surrender where there manifestly is no necessity for the use of lethal force.[134]

---

[132] ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, adopted February 26, 2009. at 996.

[133] *Id.*

[134] *Id.* at 1043.

The footnote substantiating this claim quotes the writings of Jean Pictet, once the President of the ICRC and the lead editor of the authoritative commentary of the 1949 Geneva Conventions. Pictet opined: "[i]f we can put a Soldier out of action by capturing him, we should not wound him; if we can obtain the same result by wounding him, we must not kill him. . . ."[135]

Other academics have also advanced a 'least harmful means rule.' Professor Goodman of New York University used the ICRC Interpretive Guidance as a springboard to argue a 'least harmful means rule,' "should be understood to have a solid foundation in the structure, rules, and practices of modern warfare."[136] His argument is grounded in Article 41(2) of the 1977 Additional Protocol I, which mandates the safeguarding of *hors de combat*—those combatants outside the fight.[137] Goodman argues, like the Interpretive Guidance, "a Soldier who is rendered defenseless or incapable of resistance should not be subject to attack."[138] He expands the conceptual definition of hors de combat and argues an enemy combatant should be treated like a *hors de combat* when "there is clearly no military benefit (including any risk to one's own forces) to be gained from killing rather than capturing an individual."[139] This includes situations where the enemy combatant could still physically engage in hostilities but does not. Like the Interpretive Guidance, Professor Goodman suggests that considerations of military necessity and humanity should guide the determination of how to conduct an engagement.[140] His theoretical basis for abandoning the well-entrenched rule that members of an enemy belligerency qualify as lawful objects of attack at all times and all places for as long as they remain under the operational command and control of enemy leadership and are physically capable of acting on that authority[141] is to limit the scope of

---

135 *Id.* at 1044

136 Ryan Goodman, *The Power to Kill or Capture Enemy Combatants*, 24 EUR. J. INT'L .L. 819 (2013) [*hereinafter* "Goodman"].

137 *Id.* & Additional Protocol 1, Art. 85(3).

138 Goodman, *supra* note 136, at 830.

139 *Id.* at 839.

140 *Id.*

141 Geoffrey S. Corn, Laurie R. Blank, Chris Jenks & Eric Talbot Jensen, *Belligerent Targeting and the Invalidity of a Least Harmful Means Rule*, 89 INT'L L. STUD. 536, 538 (2013) [*hereinafter* "Corn et al."].

military necessity.[142] In other words, an enemy belligerent who would do no harm; that is, defenseless, is not militarily necessary to kill.

Other academics echo this conclusion:

> [T]he current interpretation of 'necessary' as including what is less costly or less risky or even merely convenient allows too broad a discretion for forces to attack available—rather than clearly 'necessary'—targets. To bring the term 'necessary' closer to its literal meaning, it should include a least-harmful means component; it is entirely possible to conceive of 'necessary' as the least measure of harm by which to achieve a desired end.[143]

The challenges with the ICRC's rationale, along with the scholarship of Professor Goodman, are fourfold. First, there is absolutely no requirement under state practice or international law, namely the 1977 Additional Protocol of the Geneva Conventions, for a combatant to do a 'military necessity' analysis of an enemy belligerent; the Soldier need not to look to a 'least harmful means rule' as to whether the Soldier should capture the enemy belligerent or kill him. Given that military necessity "justifies those measures not forbidden by international law which are indispensable for securing the complete submission of the enemy as soon as possible,"[144] killing an enemy belligerent is *per se* permissible. The enemy belligerent takes a status under IHL of being a military target. The rationale is simple: "military necessity admits of all destruction of life or limb of armed enemies."[145] As noted Law of War expert Hays Parks concluded, "[t]here is no 'military necessity' determination requirement for an individual Soldier to engage an enemy combatant or a civilian

---

142 Goodman, *supra* note 136, at 830.

143 Gabriella Blum, *The Dispensable Lives of Soldiers*, 2 J. LEGAL ANALYSIS 115, 161 (2011).

144 *See* Note 25.

145 W. Hays Parks, *Part IX of the ICRC "Direct Participation in Hostilities" Study: No Mandate, No Expertise, and Legally Incorrect*, 42 N.Y.U. J. INT'L L. & POL. 769, 804 (2010) [*hereinafter* "Parks"].

determined to be taking a direct part in hostilities, any more than there is for a Soldier to attack an enemy tank."[146]

The second challenge is one of shifting burdens. Under current international law, the burden is on the enemy belligerent to indicate his surrender affirmatively. This assumes the enemy belligerent is not a *hors de combat*—"rendered unconscious or is otherwise incapacitated by wounds or sickness, and therefore is incapable of defending himself."[147] Professor Michael Schmitt of the Naval War College makes the point, "[a] rule that prohibits an attack whenever the individual can be captured would shift the burden from the fighter to the attacker in a way that warfighting states would have been, and remain, unlikely to countenance."[148] These States would not adhere to such a shift in burden because it would add a layer of complexity to military operations—training, implementation, accountability—that is simply unsustainable. The reality is, "the historic consequence of combat is that combatants lawfully may kill their enemies and are at constant risk of being killed by them."[149]

Related to the shifting burden States would eschew, the third troubling point about the ICRC's proposal is its lack of practicality. In the words of Professors Geoffrey Corn, Laurie Blank, Chris Jenks, and Eric Talbot Jensen:

> once the law requires that Soldiers assess the actual threat an enemy combatant poses, the inevitable consequence of a rule that requires less harmful means based on the absence of an actual threat, the effectiveness of combat capability risks dilution, and tactical clarity will be degraded. . . . [and] [d]iluting tactical clarity will inevitably dilute . . . moral clarity.[150]

---

[146] *Id.*

[147] Additional Protocol 1, Art. 41.

[148] Michael N. Schmitt, *Wound, Capture, or Kill: A Reply to Ryan Goodman's 'The Power to Kill or Capture Enemy Combatants'*, 24 EUR. J. INT'L .L. 855, 858 (2013).

[149] Parks, *supra* note 145, at 829.

[150] Corn et al., *supra* note 141, at 567-568.

Once the element of subjectivity enters the equation, moral clarity—whether it is at the tactical, operational, or strategic level—exits. Professors Corn, Blank, Jenks, and Jensen make a compelling case that not giving the Soldier the clarity of whether he can engage and shoot an enemy belligerent will result in hesitation, confusion, or create a chilling effect on what the Soldier is asked to do: engage with and destroy the enemy. The second-guessing with the benefit of 20/20 hindsight will cripple a Soldier's certainty that when he engages with the enemy, his mission, as has been the mission of Soldiers for centuries before him, is to kill the enemy. And "the assurance and knowledge that the always difficult decision to take another human life was legally and operationally justified. . . ."[151] is critical to a Soldier's mental and moral compass. The authors of this article go one step further: the 'least harmful means rule' would eviscerate moral clarity in the fog of war.

The fourth concern is that the 'least harmful means rule' is actually the conflation of two legal regimes: IHL and domestic law norms outlined within human rights law (HRL). Under HRL, known as the law enforcement regime, the use of lethal force is one of last resort. When a law enforcement officer has reasonable alternatives, he or she must exercise them. The criminal suspect in a domestic context never takes a status of a military target; in laymen's speak, the criminal cannot be killed merely because of what he is suspected of having done criminally. The compact in the law enforcement paradigm is "to protect individuals from abuse by their State"[152] of which the suspect is a member. And when lethal force is used in the domestic setting, it must be necessary, proportional, and imminent; that is, the officer triggers a right of self-defense for himself or others in the vicinity.

In the U.S. context, the Supreme Court has held that the use of deadly force is reasonable under the Constitution and therefore authorized when the officer has probable cause to believe the suspect

---

[151] *Id.* at 620.

[152] ICRC, The Use of Force in Armed Conflicts: Interplay between the Conduct of Hostilities and Law Enforcement Paradigms at 7, found at https://www.icrc.org/eng/assets/files/publications/icrc-002-4171.pdf [*hereinafter* "Interplay"].

is dangerous and can escape and a verbal warning, if feasible, is given.[153] On the other side of the equation, the Court has held that "[w]here a suspect poses no immediate threat to the officer and no threat to others, the harm resulting from failing to apprehend him does not justify the use of deadly force to do so."[154] It is the criminal's conduct that will drive the actions of the police officer. The moral compact of the officer with the society they serve is the basis for their authority: "human rights law regulates the resort to force by State authorities in order to maintain or restore public security, law and order."[155] Minimum force or a 'least harmful means rule' in this context makes sense—lethal force is a measure of last resort because of what the police officer is entrusted to accomplish.

This is not the logic behind IHL. The driving force behind IHL is not to ensure public security, although that could be one the military's tasks; the main goal is to set parameters for Soldiers as agents of the State on how to destroy the enemy. The cardinal rule of the combatant is distinction—"parties to an armed conflict must at all times distinguish between civilians and civilian objects on the one hand, and combatants and military objectives on the other hand and direct their attacks only against the latter."[156] Given this limitation on the use of force, the Soldier, as an agent of the State, is told by the State how to accomplish the goal of destroying the combatants and military objectives. The use of force to accomplish the mission is driven by the State. This collective action by the State uses the Soldier to effectuate this goal because the State tells the Soldier what are the policy limits of 'military necessity' to accomplish the mission. The role and purpose of the police officer is fundamentally different, and it is why the law enforcement paradigm is troubling in an armed conflict scenario.

153 Tennessee v. Garner, 471 U.S. 1, 12 (1985).

154 *Id.*

155 Interplay, *supra* note 152, at 7.

156 *See* note 33.

E. Trend 5: Challenging the Use of Force by the Military in Civil Courts that Lack Subject Matter Competence

Scholars and international organizations that would make it more difficult for Soldiers to engage the enemy are but one prong of the trend against the use of military force. The other prongs stem from the legal profession: one of those prongs is the access litigants have to the courtroom to challenge decisions made by military personnel. The civil litigation exposure prong is best evidenced by a string of recent cases emerging from the United Kingdom.

Article 1 of the European Convention on Human Rights (ECHR), drafted in 1950, states signatories "shall secure to everyone within their jurisdiction the rights and freedoms defined in . . . this Convention."[157] The Convention, in its first substantive article, Article 2, outlines a central pillar of human rights law: the right to life.[158] The Convention mandates that "[e]veryone's right to life shall be protected by law."[159] It does, however, give its signatories a caveat: "[d]eprivation of life shall not be regarded as inflicted in contravention of this article when it results from the use of force which is not more than absolutely necessary. . . ."[160] To judicially enforce these rights and freedoms, the convention established a court: the European Court of Human Rights (ECtHR).[161] This court, which virtually all European countries have ratified, to include the UK, can and has trumped the rulings of domestic courts.

The real battle line of when States have violated one's right to life has been the elasticity of the concept of jurisdiction; in other words, does the right to life provision contained in Article 2—or any other provision within the Convention, for that matter—have extraterritorial application outside Europe? Of particular import is whether this human rights norm applies to conflict areas like Afghanistan and Iraq. In late 2001, the case of *Bankovic et al. v. Belgium et al* was brought before the ECtHR by six citizens from the Federal

157 Article 1, European Convention on Human Rights (2010).
158 *Id.* at Article 2.
159 *Id.* at Art. 2(1).
160 *Id.* at Art. 2(2).
161 *Id.* at Art. 19-51.

Republic of Yugoslavia against 17 European members of the North Atlantic Treaty Organization (NATO).[162] The claim flowed from NATO's Operation Allied Force. This operation was an air campaign directed at Yugoslavia in an effort to force Yugoslavia to remove its forces from Kosovo.[163] In the morning raid of April 23, 1999, NATO bombs killed and injured scores of Yugoslavians.[164] The claimants, whose relatives died, alleged a violation of the right to life under Article 2.[165] The question for the ECtHR was whether there was jurisdiction to allow the case to go forward. The ECtHR said individuals killed by missiles or bombs fired from an aircraft outside an area under the effective control of a State were not within the State's jurisdiction.[166]

The defendants in the *Bankovic* Case, the 17 NATO States, argued that the term "jurisdiction" meant an "assertion or exercise of legal authority, actual or purported, over persons owing some form of allegiance to that State or who have been brought within that State's control."[167] The ECtHR seemed to agree. It proclaimed that "the jurisdictional competence of a State is primarily territorial."[168] The Court went on to articulate that "Article 1 of the Convention must be considered to reflect this ordinary and essentially territorial notion of jurisdiction, other bases of jurisdiction being exceptional and requiring special justification in the particular circumstances of each case."[169] If extra-territorial jurisdiction was to exist, then the State must militarily occupy or exercise all or some of the public powers normally to be exercised by that territory's government.[170]

---

[162] Bankovic, Stojanovic, Stoimedovski, Joksimovic and Sukovic v. Belgium, the Czech Republic, Denmark, France, Germany, Greece, Hungary, Iceland, Italy, Luxembourg, the Netherlands, Norway, Poland, Portugal, Spain, Turkey, and the United Kingdom, App. No. 52207/99, Eur. Ct. H.R. (2001), available at 41 I.L.M. 517 [*hereinafter* "Bankovic v. Belgium"].

[163] *Id.* at pp 518-519.

[164] *Id.*

[165] *Id.* at 522.

[166] *Id.* at pp. 523-524.

[167] *Id.* at 522.

[168] *Id.* at 526.

[169] *Id.*

[170] *Id.* at 528.

In other words, a fair reading of *Bankovic* is that the Convention's extraterritorial jurisdiction must be exceptional. Professor Marko Milanovic of the University of Nottingham, however, traces the ECtHR's slow abandonment of this norm.[171] In 2007, for example, the ECtHR in *Pad and others v. Turkey* found jurisdiction when an Iranian family living near the Turkish-Iranian border was killed by a missile.[172] It was disputed where the attack occurred but "the Court clearly thought that it would have been entirely arbitrary for the application of the [European Court of Human Rights] to hinge on the applicants' location within a few hundred metres."[173]

Ten years after *Bankovic*, the ECtHR heard the case of *Al-Skeini v. United Kingdom*.[174] In *Al-Skeini*, six Iraqis brought suit against the United Kingdom. The six claimants asserted the British failed to conduct a full and thorough investigation into the deaths of their family members; this, they maintained, was a procedural violation of Article 2, the right to life.[175] Five of the dead Iraqis died in fire fights with the British troops. According to the British Government, British troops were patrolling the streets of Basra one evening in August 2003 when they heard gunfire. As the Soldiers approached the gunfire, the patrol leader saw several Iraqi men, including Mr. Al-Skeini, with weapons; one of the Iraqi men pointed his weapon at him and his unit. In self-defense, the British Soldier shot and killed the Iraqi men. A subsequent investigation found that the Soldiers' actions were a valid exercise of self-defense.[176] The Iraqi testimony is starkly different: the British Soldiers killed the Iraqis without provocation and the reason one of the deceased Iraqis had a weapon was because he was walking to a funeral and discharge of weapons at

---

171 Marko Milanovic, Al-Skeini and Al-Jedda in Strasbourg, 23 EUR. J. INT'L .L. 121 (2012) [*hereinafter* "Milanovic Al-Skeini"].

172 *Id.* at 124.

173 *Id.*

174 *Id.* at 121.

175 *Id.* at 125.

176 ECtHR, *Al-Skeini et al. v. UK, App. No. 55721/07,7, 7 July 2011* at para. 34-62.

funerals is common.[177] In other words, the Iraqis maintained that those killed never threatened the British Soldiers.

The sixth claimant in *Al-Skeini* drew the most scrutiny. Like the other claimants, Mr. Baha Mousa's father, on behalf of his son, claimed that there had been an inadequate investigation. For Mr. Mousa, however, is was for the asphyxiation death of Mr. Mousa in a British detainment facility in Basra.[178]

The British House of Lords dismissed the claims of the five Iraqis involved in the firefight.[179] The majority applied an "effective control" test. The United Kingdom never exercised effective control over Basra, even though the British were an occupying power in Basra and southern Iraq. The insurgency and the limited number of British troops made effective control in Basra not possible. The Law Lords cited *Bankovic* for the notion that the mere killing of an individual does not trigger extraterritorial jurisdiction.[180] The House of Lords did find jurisdiction regarding the death of Baha Mousa, but on the grounds that a British prison was like an embassy and jurisdiction attached.[181]

The question before the ECtHR was what does "within their jurisdiction" mean: when and where do the obligations outlined in the ECHR—specifically the right to life under Article 2—apply? The ECtHR, in essence, expanded *Bankovic* and opened the jurisdictional aperture as follows:

> . . . following the removal from power of the Ba'ath regime and under the accession of the Interim Government, the United Kingdom (together with the United States) assumed in Iraq the exercise of some of the public power normally to be exercised by a sovereign government. In particular, the United

[177] *Id.*

[178] *Id.* at paras. 63-71.

[179] R (on the application of Al-Skeini and others) v. Secretary of State for Defense (2007) UKHL (2008) AC 153.

[180] *Id.* at para. 83.

[181] *Id.* at paras. 97 & 132.

> Kingdom assumed authority and responsibility for the maintenance of security in South East Iraq. In these exceptional circumstances, the Court considers that the United Kingdom, through its Soldiers engaged in security operations in Basrah during the period in question, exercised authority and control over individuals killed in the course of such security operations, so as to establish a jurisdictional link between the deceased and the United Kingdom for the purposes of Article 1 of the Convention.[182]

This holding is extraordinarily expansive and can be read to mean that when there are boots-on-the-ground Soldiers conducting security operations, the reach of the ECTHR will extend to that battlefield. Every army has "public power." One principle mission of a Soldier is to engage in security operations, especially in light of COIN operations. The *Al-Skeini* Case extends jurisdiction, allowing individual claimants to challenge the conduct of how the military conducts its operations. This ability to second-guess a military's operations will have profound impact on how a nation's military conducts its operations worldwide. But there are second and third order effects, as well. The United Kingdom felt the brunt of *Al-Skeini* in two ways: one tactical and one strategic. The claims were allowed to go forward, costing the British Government a handsome sum of money. But more fundamentally, it opened the floodgate of claimants that would challenge how the British Army does business on the battlefield. This second point was acutely realized with the case of *Smith (No. 2) v. The Ministry of Defence*.[183]

The facts of *Smith* are chilling both factually and legally—in large measure because the claimants are members of the British military.[184] The claimants alleged a violation of Article 2—right to life. They claimed the equipment they were provided while deployed to Iraq was not suitable.[185] On 15 July 2005, a British squad-sized unit

---

[182] Note 171 at paras. 143-148.

[183] R (on the application of Smith and others) v. Secretary of State for Defense (2013) UKSC 41.

[184] *Id.*

[185] *Id. at* paras. 9-12.

patrolled Al Amarah in Iraq. The vehicle used by the patrol was a "Snatch Land Rover." This vehicle had not been fitted with an electronic countermeasure to protect it from improvised explosive devises, known as IEDs. While on patrol, the Snatch Land Rover hit an IED; three Soldiers died and two were injured. Seven months later, in the same town, another Snatch Land Rover hit an IED and two more Soldiers lost their lives. The second vehicle had been outfitted with an electronic countermeasure, but there was a part missing to the system and therefore it did not work.[186]

The families of the fallen Soldiers sued Her Majesty's Government, asserting that the Ministry of Defence breached the right to life under the ECtHR because the government neglected its duty for care. The government's legal defense centered on combat immunity.[187] This legal concept, developed through case law, stands for the proposition that "while the armed forces are in the course of actually operating against the enemy, they are under no 'actionable' duty of care as defined by common law to avoid causing loss or damage to their fellow Soldiers, or indeed to anyone who may be affected by what they do."[188]

The UK Supreme Court did not agree. The salient issue before the Court was whether the European Convention on Human Rights applies extraterritorially to protect British troops abroad, to include in combat areas of operation like Iraq.[189] The Court had already answered this question in the negative. But in light of the ECtHR ruling in *Al-Skeini*, the British High Court reversed itself and made a marked departure from its precedence. The Court, in a 4-to-3 decision, allowed the claim to proceed under Article 2 of the ECtHR as its basis. The majority opinion, written by Lord Hope, took great efforts to make its legal trepidations known:

> [the battlefield] is a field of human activity which the law should enter into with great caution . . . [i]t risks undermining the ability of a state to defend itself, or

186 *Id.*

187 Id. at para.13.

188 Tugendhat, *supra* note 26, at 31.

189 *Supra* note 178.

> its interest, at home or abroad. The world is a dangerous place, and states cannot disable themselves from meeting its challenges. Ultimately democracy itself may be at risk.[190]

The Court, however, held that the claims may go forward and granted jurisdiction to the families of the fallen Soldiers to pursue their Article 2 claims. The Court found jurisdiction under these facts, but it limited jurisdiction "in connection with the planning for and conduct of military operations in situations of armed conflict which are unrealistic or disproportionate."[191] In other words, the egregious facts of this case drove the result. This 'middle ground,' a word choice of Lord Hope,[192] was a direct extension of the expansive scope of *Al-Skeini*.

Lord Hope's sentiment that "operations conducted in the face of the enemy are inherently unpredictable"[193] is a truism. This judgment allows individuals, Soldiers in this case, to question and challenge the decisions of the military's leadership. The middle ground is no ground at all. The reality must be clear: legal mission creep will occur. The law and its profession is a product of examining events after the fact—ex post facto. The profession of arms and the law that supports it under IHL are not; International Humanitarian Law is a product of using judgment before force is used. This is why Soldiers train and prepare for conflict knowing the moment they see conflict, all plans will morph once there is contact with the enemy. As Lord Hope acknowledges:

> [t]hings tend to look and feel very different on the battlefield from the way they look on such charts and images as those behind the lines may have available to them. A court should be very slow indeed to question

190 *Id.* at para. 66.
191 *Id.* at para. 76.
192 *Id.*
193 *Id.* at para. 64.

> operational decisions made on the ground by commanders, whatever their rank or level seniority.[194]

However, the door has been opened and with it, an inevitable breed of military officer who is hesitant and timid. War is foggy and unpredictable. If courts, through litigants, are allowed to second-guess military decisions that ultimately lead men and women to their deaths, then conservatism and restraint will descend upon military decisions. Both concepts are and should be an anathema to the warrior ethos.

IV. CONCLUSION

International Humanitarian Law was created so that Soldiers did not bear the responsibility of the actions of the public; it allows the Soldier to commit acts on behalf of the State that would be illegal otherwise. When we narrow what the Soldier can do, we eliminate their ability to effectuate the end of the war. The five trends discussed, if brought to fruition and taken collectively, suffocate the Soldier. They leave a Soldier virtually helpless. The advantage goes to the actor who fails to follow the rules and is asymmetric in his infliction of violence. Instead of probing how to hold the hostile civilian accountable, the trend is to impose rules on the lawful combatant that mirror what would be imposed on a police officer. The trend is pushing jurisprudence in the wrong direction. The asymmetric fighter will not change tactics, and, in fact, limiting the Soldier will embolden these fighters. Giving such a profound advantage to the enemy, limits a Soldier's ability to determine what is militarily necessary and in the process, prolongs the war and prolongs the Soldiers' exposure to harm.

Jus in bello is the evolved product of centuries of customary practice by countless military professionals. Its core principles of distinction, military necessity, and proportionality provide the proper balance between mission and humanity in an armed conflict. They are entirely separate and morally and legally distinct from the concept of

---

194 *Id.*

jus ad bellum. If properly applied, they protect the warfighter from the blending of the management of governance and the management of violence. They do not require supplement by the very dissimilar jurisprudence of traditional criminal law to properly analyze actions on the battlefield. They continually evolve, but in a careful, deliberate manner as the cost of error is too great for not only the warfighter but also the community of international States. However, because the principles are concepts rooted in the totally unique human experience, they should only be adjudicated by courts with a level of military competence and experience, not any criminal court that extends its jurisdiction in order to make a public statement about a given conflict.

Returning to our two incidents from the introduction – one in South Carolina, one in Afghanistan -- the rules that govern the two are profoundly different. In armed conflict, the three core principles of *jus in bello* in the Just War Theory are effective in analyzing the legality of Captain Kudo's decision; these principles are simply irrelevant for judging Officer Groubert's actions. For Captain Kudo's scenario, his subjective belief was that the two diggers were either Taliban or civilians directly engaged in armed conflict because they were actively planting an IED in the road. If the belief is true, they are lawful military targets and the attack would also comply with military necessity and proportionality since there is no evidence of any collateral damage to civilians. Even if it turns that Captain Kudo was incorrect and the diggers were civilian farmers, the attack would still be lawful if his belief was objectively reasonable when viewed through the eyes of a professional warfighter in a same or similar situation.

In armed conflict, unlike the law enforcement situation in South Carolina, when the attacks are done by members of uniformed military as part of an armed conflict, privileged belligerency would apply to those acts. Those privileged belligerents are authorized by the principle of military necessity to make attacks based on the status of the targeted victim as a military target. As members of a force engaged in armed conflict with the coalition, the diggers would qualify as lawful military targets. The elimination of enemy forces is an integral part of the mandate from military necessity to secure "the

complete submission of the enemy as soon as possible"[195] and thereby end the conflict. Therefore, an attack would turn on a question of proportionality: did the concrete military advantage exceed the collateral cost in terms of damage to civilian lives and property? However, it is important to limit the proportionality analysis to the facts known by the attackers at the time of the attack. Any *post hoc* judgment based upon the results of the attack is unjust. The principle of proportionality is based upon the expected concrete military advantage gained and the expected collateral damage, not the result. Even if the attackers knew that civilians would die in the attack, the attack would still be lawful if the expected military advantage outweighed the expected collateral damage to civilians.

These protection under IHL have no relevancy for Officer Groubert; his situation requires a self-defense analysis under common criminal law. Captain Kudo's situation is not nor should it be subject to the same analysis.

War is arguably the evilest practice of mankind and all of humanity should work to prevent any and all future wars. Until that day arrives, however, we must be careful to preserve and enforce all three goals of *jus in bello*. The goals of bringing about a rapid end to the conflict and limiting the cost to the belligerents are every bit as important as the goal of avoiding civilian deaths and property damage.

---

195 *See* GARY SOLIS, THE LAW OF ARMED CONFLICT, 277 (2010) (*citing* U.S. Army Field Manual 27-10, *The Law of Land Warfare*, (Washington, DC: GPO, 1956) para. 3. a. at 4).

Penn State
Journal of Law & International Affairs

2017 VOLUME 5 NO. 1

LEGAL STATUS OF DRONES UNDER LOAC AND INTERNATIONAL LAW

Vivek Sehrawat

TABLE OF CONTENTS

I. INTRODUCTION

In the twenty-first century, the use of drones in military combat operations is one of the most legally controversial issues confronting international humanitarian law (IHL) and the law of armed conflict (LOAC).[1] This article argues that drones should be treated as any other component of the United States' (U.S.)[2] arsenal. A drone can be considered to be a weapons platform or singular weapon system. This article further argues that drones indeed offer extensive and enhanced opportunities for compliance with LOAC and other relevant laws governing the use of certain weapons. Particularly, drones are well suited to execute theories of self-defense in international affairs. In fact, drones can be used for a wide variety of tasks other than kinetic operations, such as: observation and reconnaissance, intelligence collection, target acquisition, search and rescue, delivery of humanitarian aid, and transportation of equipment.[3] The appearance of new and advanced weapons in warfare is hardly a new challenge in the history of armed conflict.[4] The epic poem Mahabharatha, [200 B.C.-200 A.D.] forbids the use of 'hyper-destructive' weapons: the warrior Arjuna, observing the law of war, refrained from using the *pasupathastra*[5] because when the fight was restricted to ordinary conventional weapons, the use of

---

[1] Michael W. Lewis, *Drones and the Boundaries of the Battlefield,* 47 TEX. INT'L. L. J. 294 (2011-12).

[2] Hereinafter, United States referred to as U.S.

[3] David Turns, *Droning on: some international humanitarian law aspects of the use of unmanned aerial vehicles in contemporary armed conflicts,* CONTEMPORARY CHALLENGES TO THE LAWS OF WAR, 199 (2014).

[4] Rayan J. Vogel, *Drone Warfare and the Law of Armed Conflict,* 39 DENV. J. INT'L L. & POL'Y, 103 (2010-2011).

[5] *See generally,* Section XL, http://www.sacred-texts.com/hin/m03/m03040.htm, *Pasupathastra:* capable of destroying all beings and creation itself, this weapon should not be hurled without adequate cause; for if hurled at any foe of little might it may destroy the whole universe. In the three worlds with all their mobile and immobile creatures, there is none who is incapable of being slain by this weapon. And it may be hurled by the mind, by the eye, by words, and by the bow.

extraordinary or unconventional weapons was not even moral, let alone in conformity with religion or recognized rules of warfare.[6]

At different times in history, developments such as the crossbow, gunpowder, machine guns, tanks, airplanes, noxious gasses, nuclear bombs, and a number of other deadly inventions irreversibly changed the landscape of warfare and required combatants to reassess the laws governing armed conflict.[7] Drones have become a central instrument in armed conflict, and an increasing number of states and even non-state actors have deployed them in some way or another – although Western armies clearly have a significant technological advantage in this respect.[8] Legal scholars have expressed a variety of opinions on the use of drones.[9] On one hand, scholars argue that drones are lawful weapons under international law in a time of armed conflict, while on the other hand, critics argue that drones are being used in ways that violate international law.[10] The legality of drones has been questioned for a variety of reasons, some more grounded in fact than others, but despite this criticism there is little question that the use of drones in surveillance and combat roles is on the rise.[11]

The recent proliferation of drones has spawned intellectual debate on whether a country has the right under the LOAC and international law to unilaterally deploy these remotely controlled aircrafts abroad for military purposes. The use of drones in support of combat operations – particularly striking distant terror operatives – has become the most controversial legal topic.[12] Many of the most-frequently expressed criticisms about drones and drone warfare do not hold up well under serious scrutiny or, at any rate, there's nothing

---

[6] GRAY D. SOLIS, THE LAW OF ARMED CONFLICT: INTERNATIONAL HUMANITARIAN LAW IN WAR 7 (2010).

[7] Vogel, *supra* note 4 at 103.

[8] Ferderic Megret, *The Humanitarian Problem with Drones,* 5 UT. L. REV. 1284 (2013).

[9] Shani Dann, *Drone Strikes and IHL,* (Nov. 6, 2014) http://humanityinwarblog.com/2014/11/06/drone-strikes-and-ihl/.

[10] *Id.*

[11] Lewis, *supra* note 1, at 294.

[12] Heeyong Daniel Jang, *The Lawfulness of and Case for Combat Drones in the Fight Against Terrorism,* 2:1 NAT'L L.J. 2 (2013-2014).

uniquely different or worse about drones when compared to other military technologies.[13] Consider the most common anti-drone argument: drones kill a disproportionate number of civilian non-combatants.[14] However, drones kill fewer civilians, as a percentage of total fatalities, than any other military weapon.[15] According to the U.N.'s mission in Afghanistan (UNAMA)[16] 2012 report, the number of Afghan civilian casualties caused by the United States and its allies did not increase in 2012, in fact, they decreased by 46 percent. More specifically, civilian casualties from 'aerial attacks' fell 42 percent.[17] The UNAMA report found that drones released 506 weapons in 2012, compared to 294 from the previous year.[18] Five incidents resulted in casualties with sixteen civilians killed and three wounded, up from just one incident in 2011.[19] Even as drone attacks increased, the U.N. reported an overall decrease in civilian deaths by airstrikes with the U.S.-led coalition implementing stricter measures to prevent innocent people from being killed.[20] In another empirical report concerning drone strikes cited by The New York Times, 522 strikes have killed an estimated 3,376 militants and 476 civilians, decimating al-Qaida leadership even as the loss of innocent life intensifies anti-American sentiment in nations where strikes occur.[21] Further, according to *The Long War Journal,* an estimated 801 militant deaths in

---

[13] Rosa Brooks, *The Constitutional and Counterterrorism Implications of Targeted Killing: Hearing Before the S. Judiciary Subcomm. On the Constitution, Civil Rights, and Human Rights,* 113TH CONG., 2 (April 23, 2013) (Statement by Professor Rosa Brooks, Geo. U. L. Center), http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1114&context=cong

[14] *Id.*

[15] William Saletan, *In Defense of Drones,* SLATE, (Feb. 2013) http://www.slate.com/articles/health_and_science/human_nature/2013/02/drones.

[16] Hereinafter, U.N.'s mission in Afghanistan referred to as "UNAMA" or "UNAMA's".

[17] Saletan, *supra* note 15.

[18] Kim Gamel, *UN: Drones killed more Afghan civilians in 2012,* YAHOO NEWS, (Feb. 19, 2013) https://www.yahoo.com/news/un-drones-killed-more-afghan-civilians-2012-145931602.html?ref=gs.

[19] *Id.*

[20] *Id.*

[21] Steven Simon, *In Defense of Drones,* MSNBC (Apr. 26, 2015), http://www.msnbc.com/msnbc/defense-drones.

Pakistan occurred from U.S. drone strikes in 2010.[22] This figure is significantly higher than the 195 drone-caused deaths occurring from 2004 to 2007.'[23]

In contrast, several claims of civilian casualties caused by conventional aircrafts and weaponry have gone underreported. For example, an interview conducted by The Economist with twenty residents of the Pakistani tribal areas confirmed that many residents view individual drone strikes as preferable to the artillery barrages of the Pakistani military.[24] The residents insisted that the drones do not kill as many civilians—a view starkly at odds with mainstream Pakistani opinion.[25] An elder from North Waziristan stated, "No one dares to tell the real picture. Drone attacks are killing the militants who are killing innocent people."[26] *Jet planes, artillery attacks,* and *bombings* are the problem, not drones. Critics often assert that U.S. drone strikes are morally wrong because they kill innocent civilians.[27] This is undoubtedly both true and tragic, but nonetheless, it does not validate the arguments against drone strikes.[28] War kills innocent civilians, period.[29] But the best evidence currently available suggests that U.S. drone strikes kill fewer civilians than most other common means of warfare.[30] The operational effectiveness of drones is undisputed. Martha McSally, former fighter pilot and drone squadron commander for the U.S. Air Force, stated in her April 23, 2013 testimony to the Senate Judiciary Sub-Committee on the Constitution, Civil Rights, and Human Rights, "once a decision has been made that it is a legal and wise strategy to conduct a target strike, the [drone] platform is usually the hands-down best choice to maximize precision, persistent intelligence, responsiveness, and

---

[22] Jang, *supra* note 12.

[23] *Id.*

[24] Kenneth Anderson & Benjamin Wittes, *Three Deep Flaws in Two New Human-Rights Reports on U.S. Drone Strikes,* NEW REPUBLIC, (Oct. 24, 2013) https://newrepublic.com/article/115329/amnesty-international-human-rights-watch-drone-reports-are-flawed

[25] *Id.*

[26] *Id.*

[27] Brooks, *supra* note 13.

[28] *Id.*

[29] *Id.*

[30] *Id.*

oversight by commanders, intelligence and legal experts. It also has the benefit of minimizing civilian casualties without risk of U.S. casualties and at relatively low cost."[31] Additionally, drone pilots located in air-conditioned trailers on secure bases are far less likely to err than fighter pilots, who have to deal with numerous other factors while on missions.[32] According to one international legal expert:

> There is little reason to treat drones as distinct from other weapons systems with regard to the legal consequences of their employment. Nor is there a sound basis for heightened concern as to their use. On the contrary, the use of drones may actually, in certain cases, enhance the protections to which various persons and objects are entitled under LOAC.[33]

The use of drones must therefore be carefully weighed against the fact that it creates enemies, even as it destroys them. Under that logic, the same argument might as well be used against all airstrikes, or for that matter, artillery strikes.[34] Both of these alternatives tend to be more indiscriminate in their effects than drones.[35]

This article argues that drones should be treated as any other component of the U.S. arsenal. A drone can be considered a weapons platform or a single weapon system. In addition, this article argues that drones indeed offer extensive and enhanced opportunities for compliance with LOAC and laws governing the use of certain weapons. Particularly, drones are well-suited to execute theories of self-defense in international affairs.

---

[31] Martha McSally, *Should the United States Continue Its Use of Drone Strikes Abroad?,* PROCON.ORG, (last updated Apr. 29, 2015) http://drones.procon.org/view.answers.php?questionID=001894.

[32] Simon, *supra* note 21.

[33] MICHAEL SCHMITT, YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 313 (2010).

[34] Simon, *supra* note 21.

[35] *Id.*

The first part of the article provided a general overview of drones and their modern day implications. The second section will discuss the definition of drones and the technological capabilities of an armed drone. The third section will discuss the *legality per se* of drones as a weapon system in association with general principles of LOAC (i.e. military necessity, humanity, distinction and proportionality). In addition, the third portion will also explore the application of just war theory and its two components, *jus as bellum* and *jus in bello*. In the fourth section, this article demonstrates how effective drones can be in executing self-defense operations, illustrated by a case study of the U.S. drone strategy during the War on Terror. Generally, this article examines the legality of drone strikes under LOAC based upon the geographical location of a given target. Finally, the article will conclude by exploring military command responsibility for the violations of LOAC during drone operations and the legal status of the drone operator.

II. DRONES

The term "drone" is consistently and materially employed throughout this article, as such, there is a need to stipulate to a working definition because of the term's importance here.

A. What Exactly is a Drone?

To ensure the same basic understanding of the term from the outset, this preliminary definition should help readers in addressing the legal issues that underlie the use of drones. Categorically, "drone" refers to any unmanned, remotely-piloted, flying craft ranging from something as small as a radio-controlled toy helicopter, to the 32,000-pound, $104 million Global Hawk military drone.[36] In determining what exactly constitutes a drone under this language one considers whether the vehicle or flying craft at issue (1) flies and (2) is

[36] Kelsey D. Atherton, *Flying Robots 101: Everything You Need to Know About Drones,* POPULAR SCI. (Mar. 7, 2013*)*, http://www.popsci.com/technology/article/2013-03/drone-any-other-name.

controlled by a pilot on the ground; if the vehicle meets this criteria it falls under the everyday-language definition of drone.[37] The U.S. Army officially defines a drone as "a land, sea, or air vehicle that is remotely or automatically controlled."[38] Military drones are also referred to as Unmanned Aerial Vehicles (UAVs), Unmanned Combat Aerial Vehicles (UCAVs), or hunter-killers.[39] The history of drones is that of a watchful eye turned weapon.[40] The drone is not a projectile, but a projectile-carrying machine.[41]

B. Technology Used in Armed Drones & their Capabilities

Before learning about the legal aspects governing drones, it is important to discuss the relevant technology used in armed drones for a better understanding of their legality. The key difference between human soldiers on the ground and a drone hovering above is that humans have to distinguish and make targeting decisions instantly. In contrast, drones give commanders "tactical patience" - the ability to see, think, and act in a controlled manner. Drones are controlled by a crew often miles away from the dangers of combat, and are capable of acting as both a combatant and a combat support vehicle in the hairiest of battles.[42] Drones combine several complimentary technologies on a single platform. [43] For example, a single drone can contain highly advanced surveillance systems, live-feed video cameras, infrared cameras, thermal sensors and radar, and various types of other equipment including global positioning systems (GPS), and precision munitions.[44] The high-tech cameras on

---

[37] *Id.*

[38] *Department of defense,* DICTIONARY OF MILITARY AND ASSOCIATED TERMS 109 (Aug. 2011). (Original Gregoire Chamayou, Translated by Janet Lloyd, A THEORY OF THE DRONE 27 (2015).

[39] Lewis, *supra* note 1, at 294.

[40] GREGOIRE CHAMAYOU, A THEORY OF THE DRONE 11 (2015).

[41] *Id.*

[42] Robert Valdes, *How the Predator UAV Works,* HOW STUFF WORKS, (Apr. 1, 2004) http://science.howstuffworks.com/predator.htm.

[43] James Igoe Walsh, *The Effectiveness of Drone Strikes in Counterinsurgency and Counter terrorism Campaigns,* STRATEGIC STUDIES INSTITUTE AND U.S. ARMY WAR COLLEGE PRESS, V (Sep. 2013).

[44] *Surveillance Drones*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/issues/surveillance-drones.

drones can scan entire cities, or alternatively, zoom in and read a milk carton from 60,000 feet.[45] Surveillance data gathered by a drone can be relayed to satellites that then send it down to ground forces to help form attack strategies and identify enemy vulnerabilities.[46] Armed drones carry highly accurate missiles that have the capacity to target individuals, automobiles, and sections of structures such as rooms in a large house.[47] These missiles can be guided by the intelligence obtained by the sensors discussed above or through real-time, on-ground intelligence.[48] Drones' low profile and relative fuel efficiency combine to permit them to spend more time on target than any other manned aircraft.[49] Some military drones can stay airborne for hours or days at a time.[50] Drones also carry Wi-Fi crackers and can act as fake cell phone towers to determine a target's location or intercept texts and phone calls.[51] Given the ongoing convergence of drones and emerging technologies, it may even become possible for drones to perform facial recognition, identify behavior patterns, and monitor individuals' conversations.[52]

A typical drone is made of light composite materials to reduce weight and increase maneuverability.[53] Drones can fly at extremely high altitudes to avoid detection[54] and their navigational systems can be programmed to operate autonomously, from takeoff to landing.[55] Drones have distinct advantages over manned aircraft vehicles, cruise missiles, and Special Operations attacks.[56] The use of drones actually permits for far greater precision in targeting than

---

[45] *Id.*

[46] V. Shalem Pravas, *Aerial Assassins: Drones, Read & Digest, (*accessed Sept. 1, 2015), http://readanddigest.com/what-is-a-drone/.

[47] *Id.*

[48] Walsh, *supra* note 43.

[49] Robert Valdes, *supra* note 42.

[50] Surveillance Drones, *supra* note 44.

[51] *Id.*

[52] Chris Cole & Jim Wright, *What are drones?,* DRONE WARS U.K. (Jan. 20, 2010) wars.net/aboutdrone/" http://dronew
ars.net/aboutdrone/.

[53] Pravas, *supra* note 46.

[54] *Id.*

[55] KENNETH R. HIMES O.F.M., DRONES AND THE ETHICS OF TARGETED KILLING 12 (2016).

[56] *Id.*

most other traditional manned aircrafts.[57] Further, drones can handle what humans cannot: G-Force speed, tedium, and boredom.[58] Among the other "intrinsic benefits" of drones: they deprive the enemy of human targets; they don't get tired, thirsty, or hungry; and are relatively inexpensive.[59] In a worst-case scenario, if a drone is lost in battle military personal can simply "crack another one out of the box" and have it up in the air shortly without the trauma of casualties or the fear of pilots becoming prisoners; both of which being common concerns when more-traditional aircraft or operation failures occur.[60] Without a doubt, drones are of great benefit to the counterterrorism effort.[61]

III. THE LAW OF ARMED CONFLICT

All warfare is governed by IHL, also known as the Law of Armed Conflict (LOAC).[62]

A. What is the Law of Armed Conflict?

The LOAC comes from both customary international law and treaties.[63] Customary international law, based on a practice that nations have come to accept as legally required, establishes the traditional rules that govern the conduct of military operations in armed conflict.[64] The Law of Armed Conflict "arises from a desire among civilized nations to prevent unnecessary suffering and

---

[57] Brooks, *supra* note 13.

[58] Alan W. Dowd, *Drone Wars: Risks and Warnings*, U.S. ARMY WAR COLLEGE (2013), http://www.strategicstudiesinstitute.army.mil/pubs/Parameters/Issues/WinterSpring_2013/1_Article_Dowd.pdf.

[59] *Id.*

[60] Valdes, *supra* note 42.

[61] Himes, *supra* note 55.

[62] James Foy, *Autonomous Weapons Systems Taking the Human Out of International Humanitarian Law*, 23 DAL. J. LEGAL STUD. 47, 53 (2014).

[63] Rod Powers, *Law of Armed Conflict (LOAC),* THE RULES OF WAR, http://usmilitary.about.com/cs/wars/a/loac.htm

[64] *Id.*

destruction while not impeding the effective waging of war."[65] Indeed, modern LOAC is largely driven by humanitarian concerns.[66] As a part of public international law the LOAC regulates the conduct of armed hostilities, but only among consenting nations.[67] It also aims to protect civilians, prisoners of war, the wounded, sick, and shipwrecked.[68] The LOAC regulates, among other things, the means and methods of warfare – the weapons used and the tactics employed.[69] At its foundation, the LOAC is based on four key principles: distinction, proportionality, unnecessary suffering, and military necessity. All of which undergird the spirit and purpose of the law and drive determinations in areas such as targeting, detention, and treatment of persons.[70] The legality of drones can also be justified under the principles of weapon laws and targeting laws. The four fundamental LOAC principles are discussed in detail in the following section.

When determining the overall lawfulness of a weapon system under LOAC, there are two distinct aspects of the law that need to be analyzed: weapons law and lawful use of drones.[71] The former verifies that the weapon itself is lawful.[72] Weapon laws determine whether the use of the weapon system during hostilities might be prohibited in some manner under the law of armed conflict.[73] A weapon must satisfy two legal aspects before it may lawfully be used on a battlefield;[74] the weapon should (1) prevent unnecessary suffering, and (2) be capable of effectively distinguishing targets. The overarching principle that pertains to weapon systems is the

---

[65] *Id.*

[66] Solis, *supra* note 6, at 7.

[67] Powers, *supra* note 63.

[68] *Id.*

[69] Oren Gross*, The New Way of War: Is There a Duty to to Use Drones?*, 7 Fla. L. Rev. 1, 27 (2015).

[70] Laurie R. Blank, *After "Top Gun": How Drone strikes impact the law of war?,* U. Pa. J. Int'l L. vol. 33:3, 681 (Feb. 14, 2012).

[71] Jeffrey Thurnher, *The Law That Applies to Autonomous Weapon Systems,* 17 AM. SOC'Y OF INT'L L. 4, (January 18, 2013), https://www.asil.org /insights/volume/17/issue/4/law-applies-autonomous-weapon-systems.

[72] *Id.*

[73] *Id.*

[74] *Id.*

prohibition of superfluous injury or unnecessary suffering.[75] Weapons that cannot be directed at specific military objectives, or weaponry considered overly dangerous by nature, can violate the principle of distinction and found to be unlawful per se.[76] Moreover, even if a specific type of weapon is not unlawful per se, or is not specifically prohibited by particular treaties, governments are prohibited from improperly employing a weapon in a manner that would result in unnecessary suffering or in the targeting of civilian populations.[77] Such use is also unlawful under the relevant rules of the LOAC.[78] The two rules governing weapon laws are discussed in detail in the following section.

1. *General Principles of the LOAC.*

In this section, the principles of the LOAC will be applied to the use of drones in combat and combat support operations. This analysis falls squarely within LOAC principles. Again, the LOAC revolves around four core principles: distinction, proportionality, preventing unnecessary suffering, and military necessity. Application of any weapon depends upon these four general principles of the LOAC. Additionally, targeting law governs the circumstances of the use of lawful weapons and includes general principles of the LOAC. The following arguments help establish a basis for the conclusion that LOAC rules are sufficient to regulate drones.

(i) Distinction

"Distinction" means persons employing force must distinguish between lawful military targets (e.g., opposing combatants, equipment, or facilities), protected persons (e.g., civilians, medical personnel, chaplains, or persons who are hors de

[75] Gross*, supra* note 69.
[76] *Id.*
[77] *Id.*
[78] *Id.*

combat), property, and unlawful targets.[79] Greater awareness of the distinction principle has coincided with technological developments that enable increasingly precise targeting.[80] According to Article 48 of Additional Protocol I of the Geneva Convention,

> 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.[81]

Through its language, Additional Protocol I prohibits the use of weapons that are "of a nature to strike military objectives and civilians or civilian objects without distinction."[82]

Far from bombing entire industrial valleys or cities, which would inevitably lead to civilians being caught in the crosshairs, new technology has allowed states to be far more discriminate.[83] Indeed, the adoption of drones equipped with precision-guided munitions is the most recent improvement.[84] Drones equipped with modern imaging technologies enable operators located thousands of miles away to view details as fine as individual faces; this allows operators to distinguish between civilians and combatants far more effectively than most other weapons systems.[85] According to General (Ret.) James E. Cartwright, former Vice Chairman of the Joint Chiefs of Staff, "advances in high band-width satellite communications, sensing

---

[79] Christopher P. Toscano, *"Friend of Humans": An Argument for Developing Autonomous Weapons Systems*, 8 J. NAT'L SEC. L. & POL'Y 189 (2010).

[80] *JOHN KAAG & SARAH KREPS, DRONE WARFARE* 81 (2010).

[81] *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I),* ICRC (8 June 1977) https://www.icrc.org/ihl/4e473c7bc8854f2ec12563f60039c738/8a9e7e14c63c7f30c12563cd0051dc5c?OpenDocument,.

[82] *Rule 71,* ICRC, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule71.

[83] Kaag & Kreps, *supra* note 80, at 81.

[84] *Id.*

[85] Brooks, *supra* note 13.

technologies – particularly full motion video – combined with existing aircraft technology has allowed armed drones to emerge as the platform of choice in this counter terror mission space."[86] On April 30, 2012, CIA Director John Brennan, said, "with the unprecedented ability of remotely piloted aircraft to precisely target a military objective while minimizing collateral damage, one could argue that never before has there been a weapon that allows U.S. to distinguish more effectively between an al-Qaida terrorist and innocent civilians…[.]"[87] Therefore, because drones can effectively distinguish between targets, it can be concluded that drones meet the standard of distinction under the LOAC.

(ii) Proportionality

The LOAC principle of proportionality requires that the expected loss of civilian life and damage to civilian property incidental to attack not be excessive in relation to the concrete and direct military advantage anticipated from striking the target.[88] Article 35 of Additional Protocol I declares that "in any armed conflict, the right of the Parties to the conflict to choose methods or means of warfare is not unlimited[;]" this basic principle was officially codified by the 1907 Hague Convention, however, studies suggest that similar albeit informal principles were commonly observed by combatants prior to the Hague Convention.[89] The principle focus of proportionality seeks to minimize incidental casualties during war and operationalizes the LOAC's fundamental premise that the means and methods of attacking the enemy are not unlimited.[90] The key here is the word "incidental," meaning outside of the military target.[91] Importantly, however, the law does not prohibit all civilian deaths—

---

[86] John Brennan, *Should the United States Continue Its Use of Drone Strikes Abroad?,* PROCON.ORG (Apr. 29, 2015), http://drones.procon.org/view.answers.php?questionID=001894.

[87] *Id.*

[88] *Basic Principles of LOAC and their Targeting Implications*, CURTIS E. LEMAY CENTER, https://doctrine.af.mil/download.jsp?filename=3-60-D33-Target-LOAC.pdf (last updated Jan. 10, 2014).

[89] Blank, *supra* note 70, at 681-82.

[90] *Id.*

[91] *Id.*

and in fact accepts some incidental civilian casualties.[92] Armed drones offer the advantage of less destructive weapons and greater command and control over firing decisions. Drones can employ Hellfire missiles that weigh one-hundred pounds with a warhead of approximately thirty five pounds.[93] That is one-twentieth the size of a standard laser-guided bomb or cruise missile and less than half the size of the smallest precision ordnance dropped from conventional aircraft.[94] Proportionality inherently covers the notion to control and limit collateral damage to civilians and civilian property. This is a venerable concept. Grotius writes, "one must take care of, so far as is possible, to prevent the death of innocent persons, even by accident."[95] Even when a target is purely militant, the element of proportionality is still considered when prosecuting a target. Proportionality brings with it an obligation to consider all options when making targeting decisions: verification of the target; timing of the attack; the chosen weapon of choice; and warnings and evacuations for civilian populations.[96] Drones, with their ability to see, think, and act in a controlled manner, provide ample opportunity to consider all options before engaging a target. Drone operators, after duly considering all options and taking all mitigating maneuvers into account, are able to minimize damage to civilian life and property.

(iii) Unnecessary suffering

The principle of humanity, also commonly referred to as the principle of unnecessary suffering, aims to minimize suffering in armed conflict.[97] The core LOAC concept of unnecessary suffering, a concept created to limit damage to civilians while killing combatants, is codified in Additional Protocol 1, Article 35(2) "it is prohibited to employ weapons, projectiles and materials and methods of warfare of

---

92 *Id.*

93 Michael W. Lewis and Emily Crawrord, *Drones and Distinction: How IHL Encouraged the Rise of Drones,* 44 Geo. J. INT'L L. 1151(2012-2013).

94 *Id.*

95 *Id. at* 275.

96 *Id.*

97 Blank, *supra* note 70, at 682.

a nature to cause superfluous injury or unnecessary suffering"[98] Once a military purpose has been achieved, the infliction of further suffering is unnecessary.[99] A weapon is not banned on the ground of superfluous injury or unnecessary suffering merely because it causes great, or even horrendous suffering or injury.[100] There is nothing unique about the armaments and munitions carried by drones and used by their pilots. Thus, Alston, who served as the U.N. Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, acknowledged in his Study on Targeted Killings that, "a missile fired from a drone is no different from any other commonly used weapon, including a gun fired by a soldier or a helicopter or gunship that fires missiles."

Compliance with the principle of unnecessary suffering depends upon the kind of weapon used and the kind of suffering that it might cause. Weapons can be specifically chosen to satisfy this principle; however, compliance with the LOAC depends upon the features of the weapon used and the competency of those employing the weapon to carry out a particular mission. Also, it is difficult to determine what constitutes "unnecessary suffering" because there is no globally accepted standard.

(iv) Military Necessity

Finally, "military necessity" means that combatants may only employ force against legitimate military objectives.[101] The principle of military necessity recognizes that a military has the right to use any measures not forbidden by the laws of war that are indispensable for securing the complete submission of the enemy as soon as possible.[102] Military necessity requires combat-forces to only engage

[98] *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), supra* note 80.

[99] Blank, *supra* note 70, at 682.

[100] Solis, *supra* note 6, at 270.

[101] Toscano, *supra* note 79.

[102] Blank, *supra* note 70, at 682.

in acts necessary to accomplish a legitimate military objective.[103] It further permits the killing of enemy combatants and other persons whose death is unavoidable.[104] The principle of military necessity is a principle of controlled violence.[105] Military necessity permits the destruction of property if that destruction is imperatively demanded by the necessities of war.[106] Destruction of civilian property as an end in-itself is a violation of international law.[107] There must be a reasonable connection between the destruction of property and the overcoming of enemy forces.[108] International humanitarian law also prohibits weapon systems that cannot be directed at a specific military target.[109] Over the past few years several U.S. Government officials have confirmed that drones are an invaluable tool against Al-Qaeda, the Islamic State, Taliban, and associated terrorist forces.[110] In some areas, drones are particularly useful because of their ability to find and identify targeted persons, and then reach into territory that ground forces cannot enter due to either military or political reasons.[111] In one reported case, the United States targeted a senior Taliban official in the impenetrable border region of Pakistan while he was resting on the roof of a house with his wife and hooked up to an IV-drip for kidney problems.[112] The Taliban member was wanted for his involvement in a number of suicide bombings and the assassination of former Pakistani Prime Minister Benazir Bhutto.[113]

---

[103] ANTHONY FINN & STEVE SCHEDING, DEVELOPMENTS AND CHALLENGES FOR AUTONOMOUS UNMANNED VEHICLES: A COMPENDIUM 172 (2010).

[104] *Id.*

[105] Gross*, supra* note 69, at 28.

[106] Finn & Scheding*, supra* note 103.

[107] *Id.*

[108] *Id.*

[109] Michael N. Schmitt, *Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics*, HARVARD NAT'L SECURITY J., 10 (2013), http://harvardnsj.org/wp-content/uploads/2013/02/Schmitt-Autonomous-Weapon-Systems-and-IHL-Final.pdf.

[110] Ryan J. Vogel, *Drone Warfare and the Law of Armed Conflict,* 39 DENV. J. INT'L L. & POL'Y, 115 (2010-2011).

[111] *Id.*

[112] *Id; See also*, Peter Finn & Joby Warrick, *Under Panetta, A More Aggressive CIA,* THE WASH. POST (Mar. 21, 2010), http://www.washingtonpost.com/wpdyn/content/article/2010/03/20/AR2010032 003343.html.

[113] *Id.*

In such situations, and others like it, drone strikes offer a "definite military advantage."[114] Drones, because of advanced technology can be very precise in targeted killing. Commanders and their legal advisors have ample to make informed decision to go after a target. They can easily assess the situation, and are capable of controlling the violence.

B. Drones as Lawful Weapons

This section is intended to determine whether current weapon laws of LOAC are capable of regulating drones. In modern times, LOAC governs the choice of weapons and prohibits or restricts the use of certain weapons. Rule 71 of Customary IHL, which applies to both international and domestic conflicts, establishes the norm that the use of weapons which are indiscriminate by nature is prohibited; this norm of customary international law is applicable in both international and non-international armed conflicts.[115] In addition, many of the basic rules and specific prohibitions and restrictions on means and methods of warfare may be found in customary intentional law.[116] These restrictions can be traced back to treaties and customary international law, and are justified on the grounds that weapons which are either: (i) indiscriminate in their effect, or (ii) cause unnecessary suffering should be prohibited.[117]

The Declaration of Saint Petersburg is the first formal agreement prohibiting the use of certain weapons in war. "The Declaration to that effect adopted in 1868, which has the force of

---

[114] *Id.*

[115] Rule 71 (Weapons That Are by Nature Indiscriminate), *Customary International Humanitarian Law,* ICRC, (accessed 7 July 2015) https://www.icrc.org/customaryihl/eng/docs/v1_cha_chapter20_rul 71,

[116] Kathleen Lawand, *A Guide to Legal Review of New Weapons, Means and Methods of Warfare, Measure to implement article 36 of Additional Protocol I of 1977 (2006),* ICRC, Revised, Geneva, (accessed 22 July 2015) http://www.article36.org/wpontent/uploads/2011/12/icrc_002_0902.pdf.

[117] A.G. Houston, *Executive Series ADDP 06.4 Law of Armed Conflict,* COMMONWEALTH OF AUSTRALIA Ed. 1, 4.4, (2006) http://www.defence.gov.au/adfwc/documents/doctrinelibrary/addp/addp06.4-lawofarmedconflict.pdf.

law, confirms the customary rule according to which the use of arms, projectiles and materials of a nature to cause unnecessary suffering is prohibited."[118] Article 36 of Additional Protocol I of 1977 serves as a further reference found in international treaties for the need to carry out legal reviews of new weapons, means, and methods of warfare. The Protocol provides that:

> [I]n the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party (describes a party to any international agreement which has both signed and ratified the treaty) 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 (HCP).[119]

"Means of warfare" are weapons and weapon systems, whereas "method of warfare" refers to the tactics, techniques and procedures by which hostilities are conducted.[120] Also, international law prohibits two categories of weapons in armed conflict: indiscriminate weapons and weapons that cause unnecessary suffering.[121] The first prohibition appears in Article 51(4) of Additional Protocol I, which defines indiscriminate attacks as: (1) attacks "not directed at a specific military objective;" (2) attacks "which employ a method or means of combat which cannot be directed at a military objective;" or (3) attacks "which employ a method or means of combat the effects of which cannot be limited as required by this Protocol."[122] It is prohibited to "use weapons that are

---

[118] *Treaties and State parties to such Treaties,* DECLARATION RENOUNCING THE USE, IN TIME OF WAR, OF EXPLOSIVE PROJECTILES UNDER 400 GRAMMES WEIGHT. SAINT PETERSBURG, 29 NOVEMBER / 11 DECEMBER 1868, ICRC https://www.icrc.org/ihl/INTRO/130?OpenDocument.

[119] *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977*, TREATIES, ST., PARTIES & COMMENT. (Int'l Comm. of the Red Cross), at Article 35, *available at* https://www.icrc.org/ihl/WebART/470-750044?OpenDocument.

[120] Schmit, *supra* note 109, at 27.

[121] Blank, *supra* note 70, at 682.

[122] *Id.*

incapable of distinguishing between civilian and military targets."[123] Examples of inherently indiscriminate weapons are the rockets that Hamas and Hezbollah have fired into Israel for many years, cluster munitions, and nuclear weapons that destroy all life within the area of the detonation. [124] Additionally, weapons that cause unnecessary suffering or superfluous injury are prohibited.[125] Expanding bullets and blinding lasers offer two examples.[126] Peter Maurer, the president of the International Committee of Red Cross has stated:

> [U]nder international humanitarian law the rules of war, i.e. the set of laws governing armed conflict, drones are not expressly prohibited, nor are they considered to be inherently indiscriminate or perfidious. In this respect, they are no different from weapons launched from manned aircraft such as helicopters or other combat aircraft. It is important to emphasize, however, that while drones are not unlawful in themselves, their use is subject to international law.[127]

Therefore, it appears drones comply with the various weapon laws, however, when a drone is acting as a "weapons platform," the ordinance carried by the drone is still governed by other specific areas of weapons law. For example, if a drone is armed with chemical weapons, the applicable law is the convention on the Prohibition of the Development, Production, Stockpiling and use of Chemical Weapons and their Destruction.[128] Alternatively, if armed with 'conventional' munitions, then the general law of targeting would apply (be that treaty law, customary international law, or both).[129]

---

123 *See*, *Id.*

124 *Id.*

125 *Id.,* at 685.

126 *Id.,* at 686.

127 Peter Maurer (the president of the ICRC), *The use of armed drones must comply with laws,* ICRC, (May 10, 2013) https://www.icrc.org/eng/resources/documents/interview/2013/05-10-drone-weapons-ihl.htm.

128 M.N. SCHMITT, LOUISE ARIMATSU, & TIM MCCORMACK, YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 137 (Aug. 5, 2011), (Ian Henderson, *chapter: Civilian Intelligence Agencies and the use of Armed Drones).*

129 *Id.*

Usually, drones carry Hellfire missiles, which are not banned by any international treaty or convention and do not have any characteristics that cause unnecessary injury. By both measures of weapon laws — indiscriminate targeting and preventing unnecessary suffering— armed drones pass muster.[130]

As discussed above, a drone can have advanced technical features and extensive surveillance capabilities, and when combined with precision-guided Hellfire missile, drones should be considered a discriminate weapon system. The ability to track a target for hours, even days, before launching an attack facilitates accurate targeting and enhances the protection of civilians by allowing drone operators the ability to choose the time and place of attack with an intent of minimizing civilian casualties or damage.[131] Therefore, because armed drones can easily target pure military objectives, and have effects that can be limited, as much as possible, to military objects, drones thus meet the standards of Article 51(4) of Additional Protocol I.[132]

C. Lawful Use of Drones Under the LOAC

Drones, like any weapon, can be used for unlawful purposes, especially outside a combat zone. However, because drones are lawful weapons, the next step is to analyze their use according to the principles of the LOAC; or more particularly, the principles of distinction, proportionality, and precaution.

1. *Distinction.*

As discussed above, advanced technology places drones in a better position to distinguish between combatants and non-combatants. Historically, distinction was fairly easy; combatants wore uniforms and non-combatants did not. Now, the 'global war on terrorism' has raised new concerns because terrorists do not wear traditional uniforms, and it has become harder to distinguish between

130 Blank, *supra* note 70, at 686.
131 *Id.* at 687.
132 *Id.*

civilians and terrorists. Terrorists often take advantage of civilian populations and hide themselves among them. The situation has raised new challenges for drone operators in regards to distinction. State militaries wishing to assert compliance with a legal regime that regards human shielding and intermingling with the civilian population as unacceptable were pressured to ensure that their attacks became increasingly more discriminate and that their intelligence became more accurate.[133] The challenge found in non-state armed conflict is identifying the legitimate target. As discussed above, Article 48 of Additional Protocol I states that:

> 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.[134]

Distinction is also emphasized in Article 51(4) of Additional Protocol I:

> Indiscriminate attacks are prohibited. Indiscriminate attacks are:
>
> (a) Those which are not directed at a specific military objective;
>
> (b) Those which employ a method or means of combat which cannot be directed at a specific military objective; or
>
> (c) Those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol; and consequently, in each such case, are of a

[133] Lewis & Crawrord, *supra* note 93, at 1153.

[134] Additional Protocol I, *available at* https://www.icrc.org/ihl/4e473c7bc8854f2ec12563f60039c738/8a9e7e14c63c7f30c12563cd00.

> nature to strike military objectives and civilians or civilian objects without distinction.[135]

Furthermore, Article 85 of Protocol I declares that nearly all violations of distinction constitute "grave breaches"(foot note explaining or one brief sentence) of the Protocol, and the Rome Statute of the International Criminal Court similarly criminalizes attacks on civilians and indiscriminate attacks.[136] However, states have historically virtually ignored the principle of distinction by employing artillery, rocket launchers, and bombers in assaults on irregular forces occupying densely populated areas, resulting in tens of thousands of civilian casualties.[137] However, in order to minimize collateral damage and comply with the principle of distinction states began to employ more precise weapons than those designed to defeat a more traditional military opponent.[138] This is where drones enter the picture.[139]

The United States has consistently asserted that it complies with the LOAC in its battle against Al-Qaeda.[140] Examining how the U.S. responds to Al-Qaedas' practice of hiding amongst the civilian populations of Iraq, Afghanistan, Pakistan, and Yemen serves as a good illustration of how a state military may seek to comply with the LOAC's distinction requirements.[141] Persons who are members of an organized armed group, but dress the same as civilians, either for a lack of uniforms or specifically to blend into the civilian population for protection, are legitimate targets at all times.[142] The United State's need for more robust intelligence greatly increased the demand for drones, which were first employed in the conflict with Al-Qaeda as real-time intelligence gathering vehicles for distinction purposes.[143]

---

135 *Article 51,* Additional Protocol I, hl/WebART/470-750065" https://www.icrc.org/ihl/WebART/470-750065.

136 Blank, *supra* note 70, at 691.

137 Lewis & Crawrord, *supra* note 93, at 1152.

138 *Id.* at 1153.

139 *Id.*

140 *Id.*

141 *Id.*

142 Blank, *supra* note 70, at 692.

143 Lewis & Crawrord, *supra* note 93, at 1153.

Drones are a better option as compared to boots on ground. Drone strikes give militaries more time to analyze the situation; operators and decision makers can use the 'pattern of life' method to pursue a target (analysis, using evidence collected by surveillance cameras on the unmanned aircraft and from other sources regarding individuals and locations).[144] Further, ground forces face the challenge of distinguishing between civilians and terrorists more promptly than drones, with less situational awareness. Drones may also reduce the emotional element for the humans behind the "joy sticks" when engaging targets.[145]

2. *Proportionality*.

Proportionality is closely linked with the principle of distinction and correctly identifying objects as military and civilian.[146] For an action to be considered proportional, the anticipated military gain must exceed the anticipated damage to civilians and their property.[147] Article 51(b) of Additional Protocol I proscribes that "an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated" is disproportionate.[148] Thus, a commander must refrain from any attack in which the expected civilian casualties will be excessive in light of the anticipated military advantage gained.[149] Loss of life and damage to property *incidental* to attacks must not be excessive in relation to the concrete and direct military advantage expected to be gained.[150] The key here is the word

144 Emptywheel, *Pattern of Life drone strikes,* SHADOW PROOF, (May 7, 2010) https://shadowproof.com/2010/05/06/pattern-of-life-drone-strikes.

145 P.W. Singer, *Military Robots and the Laws of War,* NEW ATLANTIS, 25, 40-41 (Winter 2009), *available at* http://www.thenewatlantis.com/docLib/20090203_TNA23Singer.pdf/.

146 Kaag & Kreps, *supra* note 80, at 94.

147 *Id.*

148 *Id.*

149 Blank, *supra* note 70, at 682.

150 Four basic principles, LOAC (accessed March 21, 2017) http://loacblog.com/loac-basics/4-basic-principles/; *See generally*
U.S. Army Field Manual FM27-10: Law of Land Warfare.

"incidental," meaning outside of the military targets or more commonly known as "collateral damage."[151] However, if a target is purely military (i.e. no civilian component) proportionality is not a requirement.[152] Proportionality is a necessary consideration in attacks on civilians, not on combatants.[153] Proportionality brings with it an obligation to consider all options when making targeting decisions: verifying the target, timing the target, identifying the weapons used, warning and evacuating civilian populations.[154] Grotius writes, "one must take care of, so far as is possible, to prevent the death of innocent persons, even by accident."[155] According to CIA Director John Brennan:

> Compared against other options, a pilot operating this aircraft remotely, with the benefit of technology and with the safety of distance, might actually have a clearer picture of the target and its surroundings, including the presence of innocent civilians. It's this surgical precision, the ability, with laser-like focus, to eliminate the cancerous tumor called an al-Qaida terrorist while limiting damage to the tissue around it, that makes this counterterrorism tool so essential.[156]

3. *Taking Precautions*.

The principle of precaution is important because it provides constant consideration and implementation of precautionary measures that reinforces moral clarity for the warfighter thrust into terribly complex tactical and operational environments.[157] The principle of precaution can be further understood by reviewing Article 27 of the 1899 Hague Convention:

---

151 *Id.*

152 *Id.*

153 Solis, *supra* note 6, at 274.

154 Blank, *supra* note 70, at 275.

155 *Id.*

156 Brennan, *supra* note 86.

157 Geoffrey Corn, *Precautions to minimize civilian harm are a fundamental principle of the law of war,* JUST SECURITY, (July 8, 2015) https://www.justsecurity.org /24493/obligation-precautions-fundamental-principle-law-war/.

> In sieges and bombardments all necessary steps should be taken to spare as far as possible edifices devoted to religion, art, science, and charity, hospitals, and places where the sick and wounded are collected, provided they are not used at the same time for military purposes. The besieged should indicate these buildings or places by some particular and visible signs, which should previously be notified to the assailants.[158]

Also, Article 2(3) of the 1907 Hague Convention (IX) further states, "[a] commander shall take all due measures in order that the town may suffer as little harm as possible."[159] Article 57(2)(c) of Additional Protocol I mandates that those who plan or decide upon an attack "take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects."[160] Additionally, according to article 57 (3) of Additional Protocol I, "when a choice is possible between several military objectives for obtaining a similar military advantage, the objective to be selected shall be that the attack on which may be expected to cause the least danger to civilian lives and to civilian objects."[161] The primary variables of Article 57 may be identified as "the time necessary to gather and process the additional information, the extent to which it would clarify any uncertainty, competing demands on the intelligence, surveillance, reconnaissance system in question, and risk to it and its operators'.[162] Finally, according to article 58 of Additional Protocol I, the Parties to the conflict shall, to the maximum extent feasible:

---

158 *Article 27 of the 1899 Hague Convention, available* at http://avalon.law.yale.edu/19th_century/hague02.as#art27.

159 *Article 2 of the 1907 Hague Convention, available* at http://avalon.law.yale.edu/20thcentury/hague09.asp.

160 *Article 57 (2) (ii) of AP I, available* at https://www.icrc.org/applic/ihl/ihl.nsf/9ac284404d38ed2bc1256311002afd89/50fb5579fb098faac12563cd0051dd7c.

161 Article 57 (3) of AP I, *available* at https://www.icrc.org/applic/ihl/ihl.nsf/9ac284404d38ed2bc1256311002afd89/50fb5579fb098faac12563cd0051dd7c.

162 Frederik Rosén, *Extremely Stealthy and Incredibly Close: Drones, Control and Legal Responsibility,* J CONFLICT SECURITY L. (Oct. 16, 2013), http://jcsl.oxfordjournals.org/content/early/2013/10/16/jcsl.krt02.

> (a) without prejudice to Article 49 of the Fourth Convention, endeavor to remove the civilian population, individual civilians and civilian objects under their control from the vicinity of military objectives;
>
> (b) avoid locating military objectives within or near densely populated areas;
>
> (c) take the other necessary precautions to protect the civilian population, individual civilians and civilian objects under their control against the dangers resulting from military operations. This principle of avoidance (also known as "taking precautions") means that it is not enough not to intend to kill civilians while attacking legitimate targets.[163]

Indeed, a deliberate, affirmative effort has to be made not to harm civilians.[164] This may mean, for example, that certain targets ought to be attacked only during certain hours (e.g., at night, when no civilians may be around),' that some attacks may need to be conducted from a certain angle, and that advance warnings to the civilian population must be issued by the attacker prior to the strike.[165] In this regard, drone technology removes a number of classic dilemmas related to precaution. Drones leave plenty of time for the consideration and execution of precautionary steps.[166] Drones allow commanders to incorporate precautionary measures in strategy formulation, executing signature strikes, and targeted killings.[167] Hours, days, or weeks of surveillance may lie ahead of a drone attack.[168] It has been argued that there is "strong evidence that drones are better, not worse, at noncombatant discrimination."[169] The

163 Gross, *supra* note 69, at 30.
164 *Id.*
165 *Id.*
166 Rosén, *supra* note 162.
167 *Id.*
168 *Id.*
169 *Id.*

factors mentioned above do not eliminate the risk of civilian casualties, but they certainly represent feasible precautions that can minimize incidental loss of civilian life.[170] Conversely, drones may not be used when other means or methods of warfare that would result in less collateral damage with an equivalent prospect of mission success are available."[171]

The rules that govern targeting *do not turn on the type of weapon system used*, and there is no prohibition under the laws of war on the use of technologically advanced weapons systems in armed conflict--such as pilotless aircraft or so-called smart bombs—so long as they are employed in conformity with applicable laws of war.[172] In all three areas of distinction, proportionality, and precautions—drones' unique and advanced capabilities suggest great potential for adherence to LOAC obligations.[173] Drones are not automatons; they depend on human operators, analysts, and decision makers to comply with the laws of war.

D. Just War Theory

The Just War Theory formalizes the moral justifications for war.[174] It is a lens fixed in the Western philosophical tradition.[175] From the start, Just War theorists have focused on two central

---

[170] Stuart Casey-Maslen, *Drone strikes under jus ad bellum, jus in bello, and international human rights law,* 94 INT'L REV. OF THE RED CROSS, NO. 886 AT 601 (Summer 2012), https://www.icrc.org/eng/assets/files/review/2012/irrc-886-casey-maslen.pdf.

[171] Blank, *supra* note 70, at 686

[172] Galloway Family Foundation, *Lawful Use of Drones by Non-State Actors: Who can Kill,* (Jan. 8, 2014) http://www.gallowayfoundation.org/lawful-use-of-drones-by-non-state-actors-who-can-kill/.

[173] Blank, *supra* note 70, at 701.

[174] Ethan A. Wright, *Of Drones and Justice: A Just War Theory Analysis of the Unite States' Drone Campaigns,* URSINUS COLLEGE, at 12 (2015) http://digitalcommons.ursinus.edu/cgi/viewcontent.cgi?article=1003&context=ethics_essay.

[175] *Id.*

questions: (1) when is it appropriate to go to war (*jus ad bellum*), and (2) how should the war be fought (*jus in bello*).[176]

1. *Jus Ad Bellum.*

Jus ad bellum means the legality of the use of force by a territorial state. *Jus ad bellum* governs the legality of recourse to military force (including drone strikes) by one state against another, and against armed non-state actors.[177] As a threshold matter, the *jus ad bellum* inquiry depends on whether the territorial state has consented to the drone strike.[178] However, recent history has demonstrated that consent of a state is not necessarily required when conducting drone operations.[179] Article 2(4) is properly interpreted as prohibiting all uses of force above a certain minimal level.[180] Minimal uses of force such as firing a single shot across an international boundary might violate the principle of non-intervention, but is probably too minor to come within the purview of Article 2(4).[181] The threshold for the occurrence of an armed attack by another state thus appears to be relatively high, going beyond a mere frontier incident between members of the armed forces of two states (or armed groups operating in one state with limited support from another state).[182] It might even be argued by some that a very limited and targeted drone strike by one state, against individuals located in another state, would not constitute an armed attack under the UN Charter or customary law.[183] This argument is based on the highly contested concept of anticipatory self-defense (self-defense will be

176 Erich Freiberger, *Just War Theory and the Ethics of Drone Warfare,* E-INT'L REL., (July 18, 2013), http://www.e-ir.info/2013/07/18/just-war-theory-and-the-ethics-of-drone-warfare/.

177 Maslen, *supra* note 170, at 601.

178 Laurence Shore et al., *The Legality Under International Law of Targeted Killings by Drones Launched by the United States,* COMMITTEE ON INT'L L., N.Y. CITY B. ASS'N, at 8 (June 8, 2014)

179 Maslen, *supra* note 170, at 601.

180 Mary Ellen O'Connell, *Unlawful Killing with Combat Drones,* A CASE STUDY OF PAKISTAN, at 13 (2004-2009).

181 *Id.*

182 Maslen, *supra* note 170, at 602.

183 *Id.*

discussed separately in a later section).[184] If there is consent, there is no infringement on sovereignty.[185] Although a definitive answer to this factual question is impossible without access to confidential material, the publicly available information suggests that states[186] have given their consent to U.S. drone strikes.[187] Because some state have publicly withheld their consent, the U.S. must consider whether alternative justifications provide a legal basis for continued U.S. drone strikes under Just War theory.[188]

(i) Jus in Bello

Jus in bello analysis provides a legal basis for states in determining who is an acceptable target, and who is not. The typical distinction is between "combatants," who may be the targets of wartime operations, and "non-combatants," who are exempt from being targets of such attacks.[189] In essence, jus in bello is the foundation for the principles of distinction, proportionality, and necessity discussed above. Most legal scholars agree that drone strikes are legal under jus in bello as long as they occur during armed conflict.[190] Nothing is inherently illegal about using drones to kill during warfare, just as other airplanes are not forbidden.[191] Drones by themselves are not really weapons, and the armaments they do carry are generally lawful.[192]

---

184 *Id.*

185 Shore et al., *supra* note 178, at 8-9.

186 With the apparent exception of Pakistan.

187 Shore et al., *supra* note 178, at 9.

188 *Id.*

189 Freiberger, *supra* note 176.

190 JAMES DESHAW RAE, JOHN CRIST, & PALGRAVE MACMILLAN, ANALYZING THE DRONE DEBATES: TARGETED KILLINGS, REMOTE WARFARE, AND MILITARY TECHNOLOGY 62 (Mar. 12, 2014), *available* at https://books.google.com/books?id=eFkJAwAAQBAJ&pg=PA62&lpg=PA62&dq=Drones+as+Lawful+Weapons&source=bl&ots=mW3rmZwFPG&sig=-I5mkvpBXyHmv3I0_Niv_jd1l-U&hl=en&sa=X&ved=0CDwQ6AEwBGoVChMIuIHuqZHayAIVi6SICh26wwK-#v=onepage&q=Drones%20as%20Lawfu.

191 *Id.*

192 *Id.*

IV. SELF-DEFENSE THEORY

This section demonstrates the effectiveness of drones in executing self-defense operations, illustrated by a case study of the U.S. drone strategy during the War on Terror. U.S. national security strategy has encompassed the pre-emptive self-defense doctrine since the domestic attack that took place on September 11, 2001; commonly referred to as "9/11." This doctrine argues that it is legal for a state to launch a pre-emptive attack when it reasonably believes that another entity is planning an attack on the state.[193] However, the U.S. has long recognized the importance of defending its interests, both domestically and abroad. In 1854, a U.S. diplomat was attacked in the town of San Juan del Norte (Greytown)[194], Nicaragua.[195] At the time of the attack, Greytown had been forcibly seized by forces that were politically unrecognized by the U.S., and engaged in other acts of violence against U.S. nationals.[196] The U.S. Secretary of the Navy ordered the bombardment of the town after the enemy force's refusal to adhere to the U.S.'s demand for redress.[197] The presidential authorization of the military force used in Greytown was later challenged in U.S. courts, with each ruling being appealed until the case arrived at the Supreme Court.[198] Justice Nelson of the U.S. Supreme Court stated in the opinion that the President had the power to order the responsive use of armed force as part of a power of "protection" of U.S. nationals abroad against "acts of lawless violence" and "an irresponsible and marauding community."[199] At the

---

193 Kate McCann & Christopher Hope, *Are UK drone strikes in Syria legal?* THE TELEGRAPH, (Sept. 8, 2015), http://www.telegraph.co.uk/news/worldnews /middleeast/syria/11852228/Are-UK-drone-strikes- in-Syria-legal.html.

194 Hereinafter San Juan del Norte is referred as Greytown.

195 Jordan J. Paust, *Self-Defense Targeting of Non-State Actors and Permissibility of U.S. Use of Drones in Pakistan,* 19.2 J. OF TRANSNATIONAL L. & POL'Y, at 245 (*also see*, Durand v. Hollins, 8 F. Cas. 111 (C.C.S.D.N.Y. 1860) (No. 4186). Due to lack of recognition of the putative government, the community can be classified as a non-state actor).

196 *Id.*

197 *Id.*

198 *Id. at* 245.

199 *Id.*

time of the ruling, the U.S. did not consider the ongoing conflict with Nicaragua, Greytown, or its unrecognized government as "war".[200]

The customary law of a state's right to self-defense is enshrined in Article 51 of the UN Charter.[201] Article 51 states:

> [N]othing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

Article 51 of the Charter expressly affirms the right of a state to respond defensively "if an armed attack occurs."[202] "Armed attack" is the operative phrase of the text; a state may use force against both state and non-state aggressors under a theory of self-defense. And further, nothing in the language of Article 51 or any otherwise relevant customary international law requires consent of the state from which a non-state actor attack is emanating, and on whose territory a self-defense action takes place against the non-state actor.[203] Article 51 provides that nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.[204] The United States has justified its

---

200 *Id.* at 246.
201 Schmitt, *supra* note 33, at 5.
202 Paust, *supra* note 195, at 241.
203 *Id.* at 249.
204 Schmitt, *supra* note 33, at 5.

drone operations occurring outside the context of an armed conflict with another state on the basis of this right.[205]

In fact, with respect to permissible measures of self-defense under Article 51, a form of consent from each member of the United Nations already exists in advance by treaty.[206] For example, with respect to the U.S. use of drones in Pakistan to target Al-Qaeda and Taliban forces, it is clear that the U.S. would not need the express consent of Pakistan to carry out self-defense targeting.[207] It is also clear that the U.S. has the right to use drones in Pakistan under Article 51 of the Charter in self-defense to protect U.S. interests from continuous Al-Qaeda and Taliban attacks launched from Pakistan.[208] There is a growing body of law that generally recognizes the actions taken by the U.S. as legal according to international standards. According to public reports, U.S. officials have regularly consulted with Pakistani authorities when drones have been employed for strike operations in Pakistan.[209] However, Pakistan maintains only limited control over large swaths of its territory, and thus, as a result, terrorists have used that ungoverned space to their advantage; in response, President Trump and former-President Barack Obama have made clear that the United States will act if and when Pakistan cannot.[210]

V. GEOGRAPHICAL LOCATION OF DRONE STRIKES AND LOAC

Under the LOAC, in military operations, the location of a strike matters. The LOAC cannot apply places where armed conflict does not exist, and the determination of whether armed conflict does in-fact exist is based upon the intensity of the violence occurring in that given place, in addition to the level of organization employed by the forces involved, as laid out in the *Tadic* opinion.[211] The

205 *Id.*
206 Paust, *supra* note 195, at 239.
207 *Id.* at 249.
208 *Id.* at 250.
209 Vogel, *supra* note 110, at 131.
210 *Id.*
211 Lewis, *supra* note 1, at 301.

appearance of drones in the arsenal of armed conflict has stimulated renewed attempts to define the parameters of the modern battlefield.[212] The location in which military operations are actually taking place at any given time is known as the 'area of operations,' "the theatre of war," or simply, the 'battlefield.'[213] Conventional LOAC contains references to "zones of military operations," the 'zone of combat,' and 'battlefield areas' although these terms remain ambiguous.[214] The ever-increasing use of drones in the pursuit of the "war on terror" has raised concerns over the emergence of a global battlefield whereby the entire planet is subject to the application of the LOAC.[215]

For the past several years, the geographical location of drone attacks has expanded at a rapid rate; Afghanistan, Pakistan, Yemen, Somalia, and Libya have all been subject to drone strikes under the blanket justification of fighting terrorism.[216] Some of these strikes, such as those in Afghanistan, Pakistan, and Libya, fall within the generally recognized parameters of an armed conflict. Others, such as those in Yemen and Somalia, raise more complicated questions regarding where force is being used and what that means in terms of the application of the LOAC.[217] These concerns primarily stem from frequent drone strikes occurring outside the 'active battlefields' of Afghanistan and into the bordering regions of Pakistan, Yemen, and Somalia.[218]

Drone strikes blur the geographical boundaries of the battlefield. In traditional conflicts, military operations were confined to the territories of the actors and were not supposed to spillover to neutral states.[219] The law of neutrality generally "defines the relationship under international law between states engaged in an

---

[212] Noam Lubell & Nathan Derejko, *A Global Battlefield? Drones and the Geographical Scope of Armed Conflict,* 1 J. INT'L CRIMINAL JUSTICE, 8 (2013).

[213] *Id.* at 9.

[214] *Id.*

[215] *Id.*

[216] *See* Blank, *supra* note 70, at 708.

[217] *Id.*

[218] Lubell & Derejko, *supra* note 212, at 11.

[219] Blank, *supra* note 70, at 711.

armed conflict and those that are not participating in that conflict."[220] Neutrality law thus led to a geographic-based framework in which belligerents can fight on belligerent territory or the commons, but must refrain from any operations on neutral territory.[221] In essence, the battle space in a traditional armed conflict between two or more states is anywhere outside the sovereign territory of any of the neutral states.[222] However, because the U.S. drone program largely targets non-state actors that freely move across borders, laws of neutrality have become less effective.

The U.S. government operates two drone programs.[223] The military's version, which is publicly acknowledged, operates in the recognized war zones of Afghanistan and Iraq, and targets enemies of the U.S. military stationed there. As such, the program is an extension of conventional warfare.[224] The C.I.A.'s program is aimed at terror suspects around the world, including countries where U.S. troops are not based.[225] The program is classified as covert, and the intelligence agency declines to provide any information to the public about where it operates, how it selects a target, who is in charge, or how many casualties the program has led to.[226] It is contended that drone strikes in places like Yemen and Pakistan violate international law because there is no currently recognized conflict between these states and the US.[227]

However, just a few weeks after the attacks of 9/11, President George W. Bush laid the foundation for the notion of the whole world as a battlefield when he pronounced, "our war on terror will be much broader than the battlefields and beachheads of the past. This war will be fought wherever terrorists hide, or run, or plan."[228] The Obama Administration has not specifically adopted that

---

220 *Id.*

221 *Id.*

222 *Id.*

223 Mary Ellen O'Connell, *Unlawful Killing with Combat Drones, A Case Study of Pakistan*, NOTRE DAME L. SCH. LEGAL STUDIES RES. PAPER NO. 09-43, 4 (2010).

224 *Id.*

225 *Id.*

226 *Id.*

227 Lewis, *supra* note 1, at 294.

228 Blank, *supra* note 70, at 712.

same language calling for a global battlefield, but has actually significantly expanded the use of drone strikes outside of Afghanistan.[229] Al-Qaeda maintains a strong presence in a number of countries, most notably Yemen and Somalia, and uses such states to recruit, train, and plan attacks against the United States and its allies. The United States has repo1rtedly conducted limited drone operations in such countries.[230] Somalia and Yemen present an even more compelling case (than say Pakistan) of a neutral status; both states are considered "failed states" and are unable to consent or object to U.S. actions and the U.S. has not formally acknowledged the use of force in these states.[231]

However, according to Authorization for Use of Military Force (AUMF) passed by Congress in the days following 9/11:

> the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.[232]

If consent was given by a state and U.S. personnel engaged a target authorized by the AUMF, the strike would arguably be covered under AUMF authority and fall within the LOAC.[233] Therefore, the U.S. is not territorially limited when conducting operations against non-state participants.[234] Moreover, there is no question that Pakistan's territory falls within the greater AUMF theater of conflict. U.S. officials have argued that the fight with AUMF enemies is

---

229 *Id.*

230 Vogel, *supra* note 110, at 132.

231 *Id.*

232 *107th Congress,* PUBLIC LAW 107–40 (Sept. 18, 2001) http://www.gpo.gov/fdsys/pkg/PLAW-107publ40/pdf.

233 Vogel, *supra* note 110, at 132.

234 *Id.*

global, not confined to the territory of one country.[235] In fact, most of the leadership and many of the fighters intended to be covered by the AUMF are located outside of Afghanistan and within Pakistan's borders.[236]

Thus, location matters, but it is not overly prohibitive.[237] The U.S. has consistently made the case that the war with Al-Qaeda and its terrorist associates is of global reach.[238] The epicenter is in Afghanistan (and to a lesser extent Iraq), but Al-Qaeda and its offshoots, as transnational non-state actors, operate in and wage war from states across the world.[239]

VI. COMMAND RESPONSIBILITY DURING DRONE OPERATIONS

Under the LOAC and international criminal law, military personnel are criminally responsible for any war crimes they commit during war.[240] In the case of drones, the most controversial aspect of a drone program is the legal status of the operator.[241] Military commanders often consult their staff judge advocates (SJAs), especially in the escalation of conflict.[242] Seeking legal advice is increasing and has become prevalent, even in the battle space.[243] "It is also clear from the commanders . . . that legal advice is essential to effective combat operations in the current environment—legal advice is now part of the tooth not the tail."[244]

---

235 *Id.*

236 *Id.*

237 Vogel, *supra* note 110, at 132.

238 *Id.*

239 *Id.*

240 Nathalie Weizmann, *Autonomous Weapon System under International Law,* ACADEMY BRIEFING NO. 8, at 3 (Nov. 2014).

241 Vogel, *supra* note 110, at 134.

242 Edward Major, *Law and Ethics in Command Decision Making,* U. OF PENN., 61 (June 2012), *available* at https://www.law.upenn.edu/institutes/cerl/conferences/cyberwar/papers/reading/Major.pdf.

243 *Id.*

244 *Id.*

Even those who support nearly every other aspect of drone warfare find themselves uneasy with civilian personnel performing combat functions.[245] According to Peter Maurer, the president of the ICRC:

> Although the operators of remote-controlled weapons systems such as drones may be far from the battlefield, they still run the weapon system, identify the target and fire the missiles. They generally operate under responsible command; therefore, under international humanitarian law, drone operators and their chain of command are accountable for what happens. The fact of their being thousands of kilometers away from the battlefield does not absolve drone operators and their chain of command of their responsibilities, which include upholding the principles of distinction and proportionality, and taking all necessary precautions in attack. Drone operators are thus no different than the pilots of manned aircraft such as helicopters or other combat aircraft as far as their obligation to comply with international humanitarian law is concerned, and they are no different as far as being targetable under the rules of international humanitarian law.[246]

Military drone operators live and work in the US, leading relatively normal civilian lives outside of their occupation.[247] Unlike deployed personnel who remain in a combat environment continuously, drone operators maintain more stereotypical employment; they come in to work each day, gather intelligence, execute strikes when required, and return home for dinner.[248] All the while, military drone operators and their chain of command are subject to the laws of war.

---

245 Vogel, *supra* note 110, at 134.
246 Maurer, *supra* note 123.
247 Wright, *supra* note 174, at 12.
248 *Id.*

However, command responsibility is not as clearly defined when drone operations are conducted by the CIA. The CIA follows, or at least professes to follow, the laws of armed conflict.[249] As discussed above, the CIA operates one of the two drone programs for the U.S. The CIA program is not considered a military program, is not operated as one, and is not governed "by the same international protocols on the conduct of war" as the Department of Defense.[250] The clandestine and largely unaccountable nature of the CIA program creates the most ambiguities for Just War theorists.[251] According to Philip Alston U.N. Special Rapporteur on extrajudicial, summary, or arbitrary executions:

> Intelligence personnel do not have immunity from prosecution under domestic law for their conduct. They are thus unlike State armed forces which would generally be immune from prosecution for the same conduct.... Thus, CIA personnel could be prosecuted for murder under the domestic law of any country in which they conduct targeted drone killings, and could also be prosecuted for violations of applicable U.S. law.[252]

Alston is not alone in this assessment of CIA drone pilots' status. As noted by Rayan Vogel, a Foreign Affairs Specialist, and member of the Office of the Secretary of Defense and U.S. Department of Defense:

> The CIA is a civilian agency and not a branch of the U.S. Armed Forces. Even under a liberal reading of Article 4 from GC III, the CIA would not meet the requirements of lawful belligerency as a militia or volunteer corps because, while they do report to a responsible chain of command (albeit not always a military chain of command), as a group they do not wear uniforms or otherwise distinguish themselves,

---

249 Lewis & Crawrord, *supra* note 93, at 1158.

250 Wright, *supra* note 174, at 7.

251 *Id.*

252 Lewis & Crawrord, *supra* note 93, at 1158.

> nor do they carry their arms openly. CIA personnel are therefore unprivileged belligerents in this conflict.[253]

Gary Solis agrees with this assessment and has opined at some length on the status of CIA drone operators as unprivileged belligerents:

> Those CIA agents are, unlike their military counterparts but like the fighters they target, unlawful combatants. No less than their insurgent targets, they are fighters without uniforms or insignia, directly participating in hostilities, employing armed force contrary to the laws and customs of war. Even if they are sitting in Langley, the CIA pilots are civilians violating the requirement of distinction, a core concept of armed conflict, as they directly participate in hostilities...it makes no difference that CIA civilians are employed by, or in the service of, the U.S. government or its armed forces. They are civilians; they wear no distinguishing uniform or sign, and if they input target data or pilot armed drones in the combat zone, they directly participate in hostilities--which means they may be lawfully targeted .... Moreover, CIA civilian personnel who repeatedly and directly participate in hostilities may have what recent guidance from the International Committee of the Red Cross terms "a continuous combat function." That status, the ICRC guidance says, makes them legitimate targets whenever and wherever they may be found, including Langley.[254]

When the laws of armed conflict were developed, there was no technology such as drones used in the battlefield. Perhaps, new laws should be developed, especially to protect and guide drone operators. Drones are different than traditional forces that must react promptly to various hostile situations and make decisions within their

[253] *Id.* at 1159.

[254] *Id.* at 1159-60.

own judgment. In the case of drones, it is conceivable that the President may become involved with the assistance of military and legal advisors before authorizing a drone operator to engage a target. Therefore, the laws delineating command responsibility in both drone programs need to be updated and promulgated to ensure operations conform with the LOAC.

VII. CONCLUSION

This article has demonstrated that current laws are capable of governing drone warfare. The fundamental principles of the law of armed conflict, specialized weapons treaties, The Hague and Geneva conventions, customary law, and the UN Charter all provide a thorough legal backdrop to govern the usage of drones.[255] As with all weapons, it is essential to ensure that drone attacks are launched only against legitimate military objectives in accordance with the laws governing the use of force.[256] The sole legal issue specific to drone operations under both the *jus ad bellum* and the *jus in bello* is weapon choice.[257] As correctly noted by Special Reporter Alston, "a missile fired from a drone is no different from any other commonly used weapon, including a gun fired by a soldier or a helicopter or gunship that fires missiles. The critical legal question is the same for each weapon: whether its specific use complies with LOAC."[258] Drones provide a legally permissible use of force to support self-defense.[259] Drone attacks can occur against state or non-state actors located in a foreign country from which the armed attacks emanate even though there is no special consent of the foreign state, no imputation of the non-state actor's attacks to the foreign state, no armed conflict between the foreign state and the United States, and the foreign state

---

255 Vogel, *supra* note 110, at 137.

256 Blank, *supra* note 70, at 716-17.

257 Michael Schmitt, *Drone Attacks Under the Jus Ad Bellum and Jus In Bello: Clearing the 'Fog of Law',* at 13, *available* at http://ssrn.com/abstract=1801179.

258 *Id.*

259 Jordan Paust, *Operationalizing use of drones against non-state terrorists under the international law of self-defense,* 8 ALB. GOV'T L. REV., 203 (2013), (last accessed in 2015).

is willing or unable to stop the attacks.[260] However, the legal status of drone operators remains as a challenging legal question while the field continues to develop.

[260] *Id.*

Penn State
Journal of Law & International Affairs

2017 VOLUME 5 NO. 1

AIR TRAFFIC CONTROL: HOW MEXICAN CARTELS ARE UTILIZING DRONES TO TRAFFIC NARCOTICS INTO THE UNITED STATES

Britton Shields

TABLE OF CONTENTS

I. INTRODUCTION

Drone usage has been a topic of significant debate in recent years.[1] The use of drones has fostered discussions regarding their privacy implications,[2] public safety concerns,[3] and even their use to conduct military airstrikes in foreign nations.[4] However, a unique trend is emerging regarding drone use that raises novel policy concerns: recent reports have concluded that drones are now being used as a method of trafficking narcotics from Mexico into the United States.[5]

While Mexican cartels have been known to utilize creative methods when smuggling narcotics,[6] the new method of using drones

---

[1] Melanie Reid, *ARTICLE: GROUNDING DRONES: BIG BROTHER'S TOOL BOX NEEDS REGULATION NOT ELIMINATION*, 20 RICH. J.L. & TECH. 9 (2014).

[2] Robert Holly, *States Restrict Drone Use Because of Privacy Concerns*, MIDWEST CENTER FOR INVESTIGATIVE REPORTING (Mar. 21, 2014), http://investigatemidwest.org/2014/03/21/states-restrict-drone-use-because-of-privacy-concerns/.

[3] *See* Dan Loumena, *Drone crashes into stands during U.S. Open match; N.Y. teacher arrested*, LOS ANGELES TIMES (Sep. 4, 2014, 4:10 AM), http://www.latimes.com/sports/la-sp-sn-us-open-drone-crash-20150903-story.html (drone crashes into stands at sporting event); see also, Kevin Cokely, *FAA to Consider New Restrictions for Drones*, NBC DFW (Sep. 14, 2015, 11:33 PM), http://www.nbcdfw.com/news/local/FAA-to-Consider-New-Restrictions-for-Drones-327616521.html (describing a drone that nearly crashed into a private aircraft.).

[4] *See* i.e. Mehreen Zahra-Malik, *U.S. drone strike kills 15 Pakistani Taliban in Afghanistan*, REUTERS (Sep. 11, 2015, 10:54 AM), http://www.reuters.com/article/2015/09/11/us-afghanistan-drones-idUSKCN0RB1OW20150911.

[5] Nick Valencia & Michael Martinez, *Drone carrying drugs crashes south of U.S. border*, CNN (Jan. 23, 2015, 3:00 PM), http://www.cnn.com/2015/01/22/world/drug-drone-crashes-us-mexico-border/ ("U.S. authorities acknowledge a new smuggling strategy may be emerging on the border.").

[6] *Drug delivery drone crashes in Mexico*, BBC NEWS (Jan. 22, 2015), http://www.bbc.com/news/technology-30932395 ("Other methods [of smuggling] included catapults, tunnels and ultra-light aircraft.").

has important implications for a number of reasons.[7] Notably, drones are a rapidly growing industry with the potential to significantly impact the economy. Domestic use of drones in the United States is predicted to have an economic impact of over $82 billion between 2015 and 2025.[8] The demand for drones is consistently increasing among recreational users[9] and businesses,[10] causing a steady rise in their supply as well. While supply and demand continues to increase, the lack of drone regulations in the United States and Mexico is a cause for concern. Further, those regulations that currently exist do not account for the use of drones as trafficking tools at the border. It is thus unsurprising that cartels are beginning to utilize drones to traffic narcotics from Mexico into the United States.

Given the fact that the U.S.-Mexican border extends approximately 1,933 miles,[11] and that the cartels have used drones to

---

[7] Such implications include a lack of drone regulations, anti-drone security measures, and extradition issues regarding those using drones for drug trafficking between nations.

[8] Darryl Jenkins & Bijan Vasigh, *The Economic Impact of Unmanned Aircraft Systems Integration in the United States* at 2, ASSOCIATION FOR UNMANNED VEHICLE SYSTEMS INTERNATIONAL (2013).

[9] *See* Mitch Joel, *The Booming Business of Drones*, HARV. BUS. REV. (Jan. 4, 2013), https://hbr.org/2013/01/the-booming-business-of-drones (Industry analysts predict the drone market to double in less than a decade).

[10] A number of companies, including Amazon, Facebook, and Google, have invested in drone development for delivery of goods, sky-based computer networks, and even crop dusting in the agricultural community. See Jillian D'Onfro, *Why Amazon Needs Drones More Than People Realize*, BUSINESS INSIDER (July 30, 2014, 6:23 PM), http://www.businessinsider.com/amazon-drones-2014-7; John Naughton, *Why Facebook and Google are Buying Into Drones*, GUARDIAN (Apr. 19, 2014, 7:05 PM), http://www.theguardian.com/world/2014/apr/20/facebook-google-buying-into-drones-profit-motive; Mike Hanlon, *Yamaha's RMAX - The World's Most Advanced Non-Military UAV*, GIZMAG, http://www.gizmag.com/go/2440/ (last updated Nov. 19, 2004) (discussing Yamaha's R-MAX drones which are used primarily used for crop-dusting in Japan.); Jeremy Bradley, *It's one delicious drone—the Burrito Bomber*, CNN, http://www.cnn.com/2013/06/21/tech/innovation/drone-burrito-bomber/ (last updated Jun. 21, 2013, 8:35 AM) (Discussing drones to be used to deliver burritos to homes.).

[11] JANICE CHERYL BEAVER, CONG. RESEARCH SERV., RS21729, U.S. INTERNATIONAL BORDERS: BRIEF FACTS 2, (2006).

traffic narcotics an estimated 150 times per year,[12] there is a dire need for a solution to this tactic before it becomes more prevalent. This comment will focus on the rising use of drones at the border to smuggle narcotics into the United States, and suggest possible solutions to curb this new tactic being utilized by the cartels. By taking steps to solve this problem before it becomes more recurrent, the United States can hinder the use of drones as an efficient method to smuggle narcotics across the border, and in doing so, decrease the influx of narcotics trafficked into the United States. This comment will also compare the current drone regulations of Mexico and the United States with those from various other countries, and discuss how such policies can be implemented at the United States-Mexico border.

Part I of this comment has served as an introduction to the issue. Part II will briefly discuss the current state of the war on drugs at the border and how the United States and Mexico are working together to prevent the trafficking of narcotics by Mexican cartels. Part III will examine the current state of drone regulations in the United States and Mexico. Together, Parts II and III provide a background that exposes the severity of the issue of drones as trafficking tools. Finally, Part IV proposes possible solutions to prevent Mexican cartels from using drones to traffic narcotics. This section will also discuss drone regulations in several other countries, and which policies, if any, should be adopted and implemented at the border.

II. DRUG TRAFFICKING AT THE UNITED STATES – MEXICO BORDER

According to a 2013 survey, approximately 24.6 million Americans aged twelve or older (9.4 percent of the population) had used an illicit drug in the past month - a number that has steadily increased from 8.3 percent in 2002.[13] This increase in demand for

[12] *See* BBC NEWS, *supra* note 6.

[13] NATIONAL INSTITUTE ON DRUG ABUSE, DRUG FACTS: NATIONWIDE TRENDS at 1 (2015).

illicit drugs has been a catalyst for the trafficking of narcotics across the border, and has caused Mexico to become the number-one supplier of illicit drugs in the United States.[14] The majority of methamphetamine available in the United States is produced in Mexico,[15] and a 2010 report stated that ninety percent of the cocaine sold in the U.S. was transported across the border from Mexico.[16] In fact, it has been speculated that more than eighty percent of all drugs that enter the United States are trafficked across the border by Mexican cartels.[17]

A. Mexican Cartels

The competing cartels at the United States-Mexico border include the Sinaloa Cartel, the Gulf Cartel, and the Tijuana Cartel.[18] Additionally, Los Zetas provide a dominant presence in the drug violence and trafficking at the border.[19] These drug cartels control the

---

[14] S. Cody Barrus, *Interview with Mexico Drug War Expert Sylvia Longmire*, ALLTREATMENT.COM (Jan. 11, 2011), http://www.alltreatment.com/blog/2011/interview-with-mexico-drug-war-expert-sylvia-longmire/.

[15] U.S. DEPARTMENT OF JUSTICE DRUG ENFORCEMENT ADMINISTRATION, DEA-DCT-DIR-002-15, NATIONAL DRUG THREAT ASSESSMENT SUMMARY 19 (2014), available at, http://www.dea.gov/resource-center/dir-ndta-unclass.pdf; *see also* COUNTERNARCOTICS ENFORCEMENT: COORDINATION AT THE FEDERAL, STATE, AND LOCAL LEVEL: HEARING BEFORE THE SUBCOMM. ON STATE, LOCAL, AND PRIVATE SECTOR PREPAREDNESS AND INTEGRATION OF THE S. HOMELAND SEC. AND GOVERNMENTAL AFFAIRS COMM., 111th Cong. 3 (2009) (statement of John Leech, Acting Director for the Office of Counternarcotics Enforcement, U.S. Dep't of Homeland Security) ("[Mexico] is the primary source of foreign marijuana and methamphetamine, and a major source of heroin to the United States.").

[16] *See* William Finnegan, *Letter from Mexico: Silver or Lead. The Drug Cartel La Familia Gives Local Officials a Choice: Take a Bribe or a Bullet*, THE NEW YORKER, May 31, 2010, available at, http://www.newyorker.com/magazine/2010/05/31/silver-or-lead.

[17] Ginger Thompson, *U.S. Widens Its Role in Battle Against Mexico's Drug Cartels*, N.Y. TIMES, Aug. 7, 2011, available at http://www.nytimes.com/2011/08/07/world/07drugs.html?_r=0.

[18] Callin Kerr, *COMMENT: Mexico's Drug War: Is It Really a War?*, 54 S. TEX. L. REV. 193 (2012).

[19] *Id.*; *See also*, *Zetas*, INSIGHT CRIME, http://www.insightcrime.org/mexico-organized-crime-news/zetas-profile (last visited Oct. 10, 2015) (The Drug

territory surrounding the border and various drug routes it consists of, including extensive underground tunnels, waterways, roads, and walking paths.[20] While the amount of narcotics trafficked into the United States annually is difficult to quantify, it is estimated that these cartels traffic between $19 and $29 billion in drugs each year.[21] This has caused both the Mexican and United States governments to respond to the drug problem in a variety of ways.

B. Existing Statutes

1. *United States.*

A number of statutes have been enacted in both the United States and Mexico to combat the trafficking efforts of the cartels. In the United States, the Controlled Substances Act[22] prohibits any person from distributing or possessing with intent to distribute a controlled substance.[23] Additionally, 21 USC § 952 prohibits the importation of controlled substances from outside of the United States.[24] In conjunction with this statute, the Drug Enforcement

---

Enforcement Administration has described Los Zetas as "the most technologically advanced, sophisticated and violent of these paramilitary enforcement groups.").

[20] *See* Ken Stier, *Underground Threat: Tunnels Pose Trouble from Mexico to Middle East*, TIME (May 2, 2009), http://www.time.com/time/nation/article/0,8599,1895430,00.html (describing the discovery of a tunnel financed by the Tijuana Cartel that is "2,400 feet long and about nine stories deep").

[21] CNN Library, *Mexico Drug War Fast Facts*, CNN, http://www.cnn.com/2013/09/02/world/americas/mexico-drug-war-fast-facts/ (last updated Sep. 23, 2015, 4:41 PM).

[22] 21 USC § 841.

[23] Two men recently pled guilty under this statute for smuggling heroin across U.S.-Mexican border using a drone. See Kristina Davis, *Two plead guilty in border drug smuggling by drone*, Los Angeles TIMES (Aug. 12, 2015, 9:20 PM), http://www.latimes.com/local/california/la-me-drone-drugs-20150813-story.html.

[24] 21 USC § 952(a) ("It shall be unlawful to import into the customs territory of the United States from any place outside thereof (but within the United States), or to import into the United States from any place outside thereof, any controlled substance in schedule I or II of title II, or any narcotic drug in schedule III, IV, or V of title II, or ephedrine, pseudoephedrine, or phenylpropanolamine…").

Agency ("DEA") has established Federal Tracking Penalties for numerous drugs based on their quantity and schedule.[25] To further increase security at the border and help prevent the trafficking of narcotics President George W. Bush signed the Secure Fence Act in 2006.[26] The purpose of this Act was to "establish operational control over the international land and maritime borders of the United States."[27] With regard to trafficking, the Act sought to prevent the unlawful entry of narcotics and other contraband into the United States.[28] Under the Act, U.S. Border Patrol increased to approximately 20,000 agents throughout President Bush's administration, essentially doubling the number of Border Patrol agents at the time.[29] Another important statute here is 21 U.S.C. § 881, which permits the seizure and civil forfeiture of a wide variety of property associated with narcotics trafficking.[30] Relevant for purposes of this comment, this statute permits any drone used to transport narcotics to be seized by the United States. Finally, on January 25, 2017, President Donald J. Trump signed Executive Order Number 13,767: Border Security and Immigration Enforcement Improvements.[31] Under the Order, the Secretary of Homeland Security is instructed to "immediately plan, design, and construct a physical wall along the southern border"[32] in addition to hiring "5,000 additional Border Patrol agents."[33] While the main focus of the order is on immigration, it nonetheless recognizes the importance of preventing drug trafficking at the border. Given the recent nature of

---

[25] U.S. DEPARTMENT OF JUSTICE DRUG ENFORCEMENT ADMINISTRATION, FEDERAL TRACKING PENALTIES, http://www.dea.gov/druginfo/ftp3.shtml, (last visited Sep. 24, 2015).

[26] Secure Fence Act of 2006, Pub. L. No. 109-367, 120 Stat. 2638.

[27] *Id.*

[28] 120 Stat. 2638 §2(b).

[29] Bernd Debusmann, *The U.S. Border and Immigration Reform*, REUTERS (Oct. 21, 2011), http://www.reuters.com/article/2011/10/21/idUS234388556220111021.

[30] 21 U.S.C. § 881 (Property that may be seized under this statute includes the drugs themselves, materials and equipment used to make or deliver the drugs, vehicles used to transport narcotics, real property used to facilitate drug trafficking, and any firearms related to these same crimes.).

[31] Exec. Order No. 13,767, 82 Fed. Reg. 8,793 (Jan. 25, 2017).

[32] *Id.* at Sec. 4.

[33] *Id.* at Sec. 8.

this order, it remains unclear what effect it will have on narcotics trafficking into the United States.

2. *Mexico.*

In Mexico, the predominant source of the Country's drug laws is the Federal Criminal Code.[34] Article 194 of the Code provides a twenty-five year prison sentence for the production, transportation, trafficking, sale, and supply of narcotics.[35] Additionally, the Federal Law Against Organized Crime, which was approved in 1996, increased sentences for any crime committed as part of a criminal conspiracy.[36] This law also established the concept of "preventative detention," which has since been incorporated into Mexico's constitution.[37] "Preventative detention" allows for the detention of individuals on the basis of having suspected links to organized crime.[38] Suspected individuals may be detained for up to 80 days without an arrest warrant or charge.[39] Despite these laws, various critics believe the Mexican judicial system has failed to adequately address the crime and violence the nation faces at the border.[40] In particular, Mexico's judicial system has been characterized as corrupt,[41] and generally weaker than the other branches of the

---

[34] Código Penal Federal [CPF] [Federal Criminal Code], *as amended*, Diario Oficial de la Federación [DO], 14 de Agosto de 1931 (Mex.).

[35] *Id.* art. 194.

[36] Ley Federal Contra la Delincuencia Organizada [LFCDO] [Federal Law Against Organized Crime], *as amended*, Diario Oficial de la Federación [DO] 7 de Noviembre de 1996 (Mex.).

[37] *Mexico*, DRUG LAW REFORM IN LATIN AMERICA - TNI, http://www.druglawreform.info/country-information/mexico/item/205-mexico#2 (last visited Oct. 10, 2015).

[38] *Id.*

[39] *Id.*

[40] Deborah M. Weissman, *The Political Economy of Violence: Toward an Understanding of the Gender-Based Murders of Ciudad Juarez*, 30 N.C. J. INT'L L. & COM. REG. 795, 808 (2005) (discussing the failure of the Mexican legal system to respond to the murders of women in Ciudad Juarez).

[41] Human Rights Watch, *Mexico*, in WORLD REPORT 380 (2015), available at http://www.hrw.org/sites/default/files/reports/wr2015_web.pdf. ("The criminal justice system routinely fails to provide justice to victims of violent crimes and

Mexican government.[42] The threat posed by narcotics trafficking at the border, in addition to the weak response by the Mexican government, has caused the United States and Mexico to begin working in a cooperative manner to address drug-related crime at the border.

C. Cooperation Between United States and Mexico

The United States and Mexico signed an extradition treaty that went into effect in 1980.[43] The objective of this treaty is "to cooperate more closely in the fight against crime and, to this end, to mutually render better assistance in matters of extradition."[44] While this treaty provides a general means for the nations to cooperate in matters of extradition, the principal policy between the United States and Mexico with respect to cartel drug trafficking and violence is the Merida Initiative.[45] This initiative is described as a "partnership between the United States and Mexico to fight organized crime and associated violence while furthering respect for human rights and the rule of law."[46] The Merida Initiative contains four pillars: (1) Disrupt Organized Criminal Groups; (2) Strengthen Institutions (e.g., the judicial sector); (3) Build a 21st Century Border; and (4) Build Strong and Resilient Communities.[47] Under the Merida Initiative, the United States has provided over $2.3 billion in aid to Mexico, and $1.4 billion in equipment and training.[48] Such equipment includes

human rights violations. Causes of this failure include corruption, inadequate training and resources, and the complicity of prosecutors and public defenders.")

[42] *See* Matthew C. Ingram et al., *Assessing Mexico's Judicial Reform*, TRANS-BORDER INSTITUTE 4 (2012), available at http://justiceinmexico.files.wordpress.com/2010/07/tbi-assessing-judicial-reform1.pdf.

[43] Extradition Treaty Between the United States and Mexico, U.S.-Mex., May 4, 1978, T.I.A.S. No. 9656: 31 UST 5059.

[44] *Id.*

[45] U.S. Dep't of State, Bureau of Int'l Narcotics and Law Enforcement Affairs, Merida Initiative (2012), available at https://www.state.gov/j/inl/merida/.

[46] *Id.*

[47] *Id.*

[48] U.S. Embassy & Consulates in Mexico, *The Merida Initiative - Overview*, https://mx.usembassy.gov/our-relationship/policy-history/the-merida-initiative/ (last visited Feb. 3, 2017).

helicopters, surveillance equipment and military gear.[49] The funds appropriated to strengthen institutions under the second pillar focus primarily on strengthening Mexico's justice system and the aforementioned problems that plague it.[50] This is accomplished through the training of prosecutors, defenders, investigators, and forensic experts, and through judicial exchanges and partnerships between Mexican and U.S. law schools.[51] The U.S. State Department has claimed that the initiative is responsible for the removal of key drug trafficking organization leaders, the seizure of tens of thousands of tons of illicit drugs, millions in currency, and tens of thousands of weapons.[52]

D. Drone Use at Border

Though the use of drones to traffic narcotics across the border is a relatively new tactic, the United States government has been utilizing drones at the border for nearly a decade.[53] In particular, the United States Customs and Border Protection ("CBP") operates ten unmanned aircrafts ("UAs") for border surveillance and law enforcement purposes.[54] The unmanned aircrafts conduct reconnaissance missions to gather data and intelligence on drug trafficking and specific individuals either crossing the border illegally,

---

[49] *See* William A. Fix, Kendra J. Harris & Aida A. Montanaro, *Offense, Defense, or Just a Big Fence? Why Border Security is a Valid National Security Issue: St. Mary's University School of Law Center for Terrorism Law*, 14 SCHOLAR 741, 756 (2012).

[50] The Merida Initiative, *supra* note 45; see also Eric Olson, *Six Key Issues in U.S.-Mexico Security Cooperation*, WILSON CTR. (2008), available at http://www.wilsoncenter.org/sites/default/files/six_issues_usmex_security_coop.pdf.

[51] *Id.*

[52] *See* Press Release, U.S. Dep't of State, United States-Mexico Security Partnership: Progress and Impact (Mar. 23, 2010) (on file with Office of the Spokesman).

[53] Arthur Holland Michel, *Customs and Border Protection Drones*, CENTER FOR THE STUDY OF THE DRONE (Jan. 7, 2015), http://dronecenter.bard.edu/customs-and-border-protection-drones/.

[54] U.S. DEPARTMENT OF HOMELAND SECURITY, DHS/CBP/PIA-018, PRIVACY IMPACT ASSESSMENT FOR THE AIRCRAFT SYSTEMS 2 (2013), available at, http://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-aircraft-systems-20130926.pdf.

or seeking to smuggle narcotics and other contraband into the United States.[55] These efforts have been met by mild success, with unmanned aircrafts helping to seize 7,600 pounds of marijuana worth $19.3 million in 2012.[56] While the CBP originally intended to expand their number of drones to twenty-four at an additional $443 million,[57] the Department of Homeland Security has recently published a report stating that the CBP drone program has not performed to expectations and is not worth the cost to maintain.[58] In light of this report, it is unlikely that the CBP drone program will realize its projected expansion.[59] Given the fact that the United States has been implementing the use of drones in its efforts to detect drug trafficking at the border, it is unsurprising that the cartels are attempting to level the playing field by utilizing drones in their drug trafficking efforts. With this brief background on the status of drug trafficking at the border, we turn now to the current state of drone regulations in Mexico and the United States.

III. DRONE REGULATIONS IN THE UNITED STATES AND MEXICO

A. Drone Regulations in the United States

Though public drone use is a relatively new phenomenon, the foundation for drone regulations in the United States was set in 1958

---

[55] *Id.*

[56] Brian Bennett, *Predator Drones Have Yet to Prove Their Worth on Border*, LOS ANGELES TIMES (Apr. 28, 2012), http://articles.latimes.com/2012/apr/28/nation/la-na-drone-bust-20120429.

[57] Andrew Becker, *Border agency looks to expand drone fleet*, CALIFORNIA WATCH (Nov. 19, 2012), http://californiawatch.org/dailyreport/border-agency-looks-expand-drone-fleet-18678.

[58] U.S. DEPARTMENT OF HOMELAND SECURITY, OIG-15-17, U.S. CUSTOMS AND BORDER PROTECTION'S UNMANNED AIRCRAFT SYSTEM PROGRAM DOES NOT ACHIEVE INTENDED RESULTS OR RECOGNIZE ALL COSTS OF OPERATIONS (2014), available at, https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-17_Dec14.pdf.

[59] *Id.* at 1 ("The $443 million CBP plans to spend on program expansion could be put to better use by investing in alternatives, such as manned aircraft and ground surveillance assets.").

with the passage of the Federal Aviation Act.[60] This act established the Federal Aviation Administration ("FAA"), which oversees all aspects of American civil aviation and is responsible for "the safe and efficient use" of the National Airspace System.[61] Consequently, the FAA is the regulatory agency responsible for administering drone regulations in the United States.[62]

The principal piece of drone legislation applicable in the United States is the Federal Aviation Administration Modernization and Reform Act of 2012 ("'FAA Modernization and Reform Act").[63] This Act directed the FAA "to safely accelerate the integration of civil unmanned aircraft systems into the national airspace system" by September 30, 2015.[64] In other words, the FAA has been tasked with providing comprehensive drone regulations for various classes of drone users. The FAA missed this September deadline, however, and the deadline was extended into 2016.[65] The extension of the FAA Modernization and Reform Act will be of paramount importance in combatting cartel drone use, as will be discussed in Part IV.

"The United States Government has exclusive sovereignty of airspace of the United States."[66] The FAA Modernization and Reform Act directs the FAA to implement three classifications of

---

[60] Federal Aviation Act, Pub. L. 85-726, 72 Stat. 731.

[61] *Id.*

[62] A federal statute specifies the general policy of the Department of Transportation. See 49 U.S.C. § 40101. The primary purpose of the FAA (today a part of the Department of Transportation) is to maintain safety "as the highest priority in air commerce."

[63] FAA Modernization and Reform Act of 2012, Pub. L. 112-95, 126 Stat. 11 [*hereinafter* "FAA Modernization and Reform Act"].

[64] FAA Modernization and Reform Act of 2012, Pub. L. 112-95, § 332, 126 Stat. 11, 73.

[65] *See* Aviation Pros, *ARSA on FAA Extension: Time is Not on Our Side*, AVIATION PROS (Sep. 29, 2015), http://www.aviationpros.com/press_release/12120302/arsa-on-faa-extension-time-is-not-on-our-side; see also Mark Rockwel, *FAA looks to 2016 for drone rules*, 1105 MEDIA, INC. (Sep. 30, 2015), https://fcw.com/articles/2015/09/30/faa-drones.aspx ("A June 2014 Department of Transportation Inspector General report stated the agency would miss the 2015 mark because of 'significant technological barriers,' including detection and standardized air traffic procedures and other issues.").

[66] 49 U.S.C. § 40103(a).

drones into this airspace: public, civil, and model/recreational.[67] Public drones are those owned and used by the United States government or the government of a state.[68] Civil drones are all other drones not used by the government, but are not recreational.[69] Model or recreational drones are those that are flown by the general public strictly for hobby or recreational use.[70] Of these three categories, only public drones currently require certification from the FAA. It is important to note that while the FAA Modernization and Reform Act establishes the aforementioned categories of drones, as of August 29, 2016, the FAA has implemented regulations that simply govern the use of "small" drones – those weighing less than 55 pounds.[71] As a result, civil drones and model/recreational drones are currently treated in a similar manner (with minor exceptions for pilots), and can be flown without FAA certification, as long as the drone is registered and as long as those piloting them abide by the flight regulations expressed by the Small Unmanned Aircraft Rules.[72]

1. *Public (Governmental) Drones.*

A number of qualifications must be met before a drone or aircraft can qualify for public status.[73] "Whether an operation qualifies as a public aircraft operation is determined on a flight-by-flight basis, under the terms of the statute."[74] Factors taken into consideration when determining public status include ownership, the

[67] FAA Modernization and Reform Act, *supra* note 63.

[68] 49 U.S.C. § 40102(a)(41) (Operators of public aircrafts include DOD, DOJ, DHS, NASA, NOAA, state/local agencies and qualifying universities.).

[69] 49 U.S.C. § 40102(a)(16).

[70] FAA Modernization and Reform Act of 2012, Pub. L. 112-95, §336(c), 126 Stat. 11, 77-78.

[71] U.S. DEPARTMENT OF TRANSPORTATION FEDERAL AVIATION ADMINISTRATION, SUMMARY OF SMALL UNMANNED AIRCRAFT RULE (PART 107), available at https://www.faa.gov/uas/media/Part_107_Summary.pdf (last visited Feb. 9, 2017).

[72] 14 CFR 107.

[73] 49 U.S.C. § 40125.

[74] U.S. DEPARTMENT OF TRANSPORTATION FEDERAL AVIATION ADMINISTRATION, UNMANNED AIRCRAFT SYSTEMS: PUBLIC OPERATIONS (GOVERNMENTAL), available at http://www.faa.gov/uas/public_operations/ (last visited Nov. 14, 2015).

operator, the purpose of the flight, and the persons on board the aircraft.[75] A drone that qualifies as public must apply for a Certificate of Waiver or Authorization ("COA") from the FAA.[76] If the COA is issued, public agencies and organizations are then permitted to operate a particular aircraft or drone, for a particular purpose, in a particular area.[77] It should be noted that a public drone operator using the drone in an active, restricted, prohibited or warning area airspace needs permission from the entity controlling that airspace to operate the drone in the secured area.[78] Alternatively, if the governmental drone chooses to fly under the small UAS rules, it need not obtain a COA so long as it follows all rules established under 14 CFR part 107.[79]

2. *Civil Drones.*

Perhaps the most important category for purposes of this comment, civil drones are all drones that are not public or recreational. This includes drones used by businesses for commercial purposes. Currently, there are three methods of gaining FAA authorization to fly civil drones. First, a civil drone that weighs less than 55 pounds must be registered with the FAA, and the pilot of such a drone must meet certain requirements.[80] Specifically, the pilot of a civil drone must be at least 16 years old, pass an initial aeronautical knowledge test, and be vetted by the Transportation

[75] 49 U.S.C. § 40125, *supra.*

[76] U.S. DEPARTMENT OF TRANSPORTATION FEDERAL AVIATION ADMINISTRATION, CERTIFICATES OF WAIVER OR AUTHORIZATION (COA), available at https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/systemops/aaim/organizations/uas/coa/ (last visited Feb. 3, 2017).

[77] *Id.*

[78] FAA, Interim Operational Approval Guidance 08-01: Unmanned Aircraft Systems Operations in the U.S. National Airspace System 5 (2008).

[79] U.S. DEPARTMENT OF TRANSPORTATION FEDERAL AVIATION ADMINISTRATION, UNMANNED AIRCRAFT SYSTEMS: BEYOND THE BASICS, available at https://www.faa.gov/uas/beyond_the_basics/#55 (last visited Feb. 9, 2017).

[80] U.S. DEPARTMENT OF TRANSPORTATION FEDERAL AVIATION ADMINISTRATION, UNMANNED AIRCRAFT SYSTEMS: FLY FOR WORK/BUSINESS, available at https://www.faa.gov/uas/getting_started/fly_for_work_business/ (last visited Feb. 9, 2017).

Safety Administration (TSA).[81] Further, civil drones under 55 pounds are subject to various operating rules, however all are subject to waiver.[82] Second, if the civil drone exceeds 55 pounds, the drone operator must petition for an exemption under section 333 of the Modernization and Reform Act.[83] According to the FAA, a section 333 exemption "provides operators who wish to pursue safe and legal entry into the NAS a competitive advantage in the UAS marketplace, thus discouraging illegal operations and improving safety."[84] Third, civil drone operators can obtain a Special Airworthiness Certificate ("SAC").[85] To obtain such a certificate, the drone must conform to the same airworthiness standards as that of any other type of aircraft.[86] Additionally, applicants must be able to describe a number of details regarding the drone and the anticipated flight pattern.[87] It

---

[81] *Id.*

[82] *Id.* Operating rules include flying in a Class G airspace, under 400 feet, during the day, at or below 100 mph, and not over people or from a moving car.

[83] U.S. DEPARTMENT OF TRANSPORTATION FEDERAL AVIATION ADMINISTRATION, UNMANNED AIRCRAFT SYSTEMS: BEYOND THE BASICS, available at https://www.faa.gov/uas/beyond_the_basics/#55 (last visited Feb. 9, 2017).

[84] U.S. DEPARTMENT OF TRANSPORTATION FEDERAL AVIATION ADMINISTRATION, UNMANNED AIRCRAFT SYSTEMS: SECTION 333, available at https://www.faa.gov/uas/beyond_the_basics/section_333/ (last visited Feb. 9, 2017).

[85] U.S. DEPARTMENT OF TRANSPORTATION FEDERAL AVIATION ADMINISTRATION, SPECIAL AIRWORTHINESS CERTIFICATION: CERTIFICATION FOR CIVIL OPERATED UNMANNED AIRCRAFT SYSTEMS (UAS) AND OPTIONALLY PILOTED AIRCRAFT (OPA), available at https://www.faa.gov/aircraft/air_cert/airworthiness_certification/sp_awcert/experiment/sac/ (last visited Feb. 9, 2017).

[86] Brandon Bellow, COMMENT: *FLOATING TOWARD A SKY NEAR YOU: UNMANNED AIRCRAFT SYSTEMS AND THE IMPLICATIONS OF THE FAA MODERNIZATION AND REFORM ACT OF 2012*, 78 J. Air L. & Com. 585, 601 (2013).

[87] U.S. DEPARTMENT OF TRANSPORTATION FEDERAL AVIATION ADMINISTRATION, UNMANNED AIRCRAFT SYSTEMS: CIVIL OPERATIONS (NON-GOVERNMENTAL), available at http://www.faa.gov/uas/civil_operations/ (last visited Nov. 14, 2015) ("must be able to describe how their system is designed, constructed, and manufactured, including engineering processes, software development and control, configuration management, and quality assurance procedures used, along with how and where they intend to fly."); see also *Civil Flight Operations (Non-Governmental)*, B4UDRONE, available at http://b4udrone.us/civil-operations/ (last visited Feb. 9, 2017) .

should be noted that civil drones may also receive a SAC in the experimental category to perform research and development, crew training, and market surveys.[88] However, unlike other civil drones, carrying persons or property for compensation with an experimental SAC is strictly prohibited.[89]

3. *Model or Recreational Drones*.

The FAA has enacted regulations requiring the registration of all drones between 0.55 and 55 pounds, even if used for recreational purposes.[90] Those registering small recreational drones must be a U.S. citizen or legal permanent resident at least 13 years old.[91] The failure to register such a drone may result in civil and criminal penalties.[92] In addition to the federal registration process, operators of these drones must comply with a number of additional "small unmanned aircraft rules."[93] Specifically, all flights must occur during daylight, at or below 400 feet, may not exceed 100 mph, and the drone must be kept within sight of the pilot at all times.[94] Further, drones are prohibited from carrying hazardous materials or being operated in a reckless manner.[95] If a drone operator abides by these regulations, the pilot does not need FAA authorization to operate their drone. It should be noted however, that similar to civil drones, to fly a drone that weighs 55 pounds or more, operators must file for a Section 333

[88] 14 CFR §21.191.

[89] 14 CFR § 91.319(a)(2).

[90] U.S. DEPARTMENT OF TRANSPORTATION FEDERAL AVIATION ADMINISTRATION, UNMANNED AIRCRAFT SYSTEMS: REGISTRATION, available at https://www.faa.gov/uas/registration/ (last visited Feb. 3, 2017).

[91] U.S. DEPARTMENT OF TRANSPORTATION FEDERAL AVIATION ADMINISTRATION, UNMANNED AIRCRAFT SYSTEMS: FLY FOR FUN, available at https://www.faa.gov/uas/getting_started/fly_for_fun/ (last visited Feb. 9, 2017).

[92] U.S. DEPARTMENT OF TRANSPORTATION FEDERAL AVIATION ADMINISTRATION, SMALL UNMANNED AIRCRAFT SYSTEM (SUAS) REGISTRATION SERVICE, available at https://registermyuas.faa.gov (last visited Feb. 9, 2017).

[93] 14 CFR 107.

[94] U.S. DEPARTMENT OF TRANSPORTATION FEDERAL AVIATION ADMINISTRATION, SUMMARY OF SMALL UNMANNED AIRCRAFT RULE (PART 107), available at https://www.faa.gov/uas/media/Part_107_Summary.pdf (last visited Feb. 9, 2017).

[95] *Id.*

exemption.[96] Despite these limited provisions, "[n]othing in this section shall be construed to limit the authority of the Administrator to pursue enforcement action against persons operating model aircraft who endanger the safety of the national airspace system."[97]

4. *Additional Regulations*.

In addition to the above regulations, the government may classify airspace as prohibited, meaning "[n]o person may operate an aircraft within [the] area unless authorization has been granted by the using agency."[98] Additionally, foreign aircrafts, not part of the armed forces of a foreign country, may not navigate in the United States absent, among other factors, authorization from the Secretary of Transportation.[99] Finally, various criminal penalties have been put in place for violations of registration requirements in connection with transporting a controlled substance by aircraft.[100]

B. Drone Regulations in Mexico

Mexico's drone regulations are provided in the Dirección General de Aeronáutica Civil (General Direction Manual of Civil Aeronautics). The Dirección General de Aeronáutica Civil is a part of the Secretariat of Communications and Transportation of Mexico ("Secretariat"), which in essence is Mexico's Transportation Department.[101] The Secretariat is responsible for enacting drone regulations in Mexico, which has been accomplished principally

---

[96] U.S. DEPARTMENT OF TRANSPORTATION FEDERAL AVIATION ADMINISTRATION, UNMANNED AIRCRAFT SYSTEMS: BEYOND THE BASICS, available at https://www.faa.gov/uas/beyond_the_basics/#55 (last visited Feb. 9, 2017).

[97] FAA Modernization and Reform Act of 2012, Pub. L. 112-95, §336(b), 126 Stat. 11, 77.

[98] 14 CFR § 73.83.

[99] 49 USCS § 41703.

[100] 49 USCS § 46306.

[101] *See generally*, Secretaría de Comunicaciones y Transportes, http://www.sct.gob.mx (last visited Feb. 3, 2017).

through revisions to Mexico's Aviation Law, COAV23-10R2, in May 2015.[102]

COAV23-10R2 defines a drone as any vehicle capable of "transiting through air space."[103] The most important provisions within this regulation regarding drones are the drone classifications and the no permit requirement for the operation of small drones in daylight.[104] Specifically, the regulation divides drones into three categories based on size: small-sized drones weighing 2 kilograms (4.4 pounds) or less; medium-sized drones weighing between 2 kilograms and 25 kilograms (55 pounds); and large-sized drones weighing over 25 kilograms.[105] Small-sized drones are typically those used by hobbyists, and, as stated above, do not require any permit to fly, so long as they abide by the general flight laws.[106] Medium-sized drones require a permit to operate, unless operated on the grounds of a flight club.[107] Finally, large-sized drones require an operating permit, and the operator must also be a licensed pilot.[108]

Notwithstanding the above categorizations of drones, small recreational drones must abide by a number of additional regulations. For example, all drone flights must be operated during daylight hours only.[109] Additionally, all drones must stay 9.2 kilometers (5.72 miles) away from airports and 900 meters (0.56 miles) from helicopter pads. Further, small-sized drones are prohibited from flying above 122 meters (400 feet).[110] Throughout the duration of the flight, the

---

[102] CO AV-23/10 R2, available at http://www.sct.gob.mx/fileadmin/DireccionesGrales/DGAC/00-aeronautica/co-av-23-10-r2.pdf.

[103] *Id.*

[104] *See* Nancy Palencia, *Mexico drones get green light*, CAPITALMEDIA, available at http://thenews.mx/2015/04/mexico-drones-get-green-light (last visited Nov. 12, 2015).

[105] CO AV-23/10 R2, art. 7, p. 4, available at http://www.sct.gob.mx/fileadmin/DireccionesGrales/DGAC/00-aeronautica/co-av-23-10-r2.pdf.

[106] *Id.* at art. 8, p. 5.

[107] *Id.* at art. 9, p. 6.

[108] *Id.* at art. 10, p. 6.

[109] *Id.* at art. 7.2(k); see also *Mexico Drone Laws*, UAV SYSTEMS INTERNATIONAL INC. (Nov. 1, 2015), https://uavsystemsinternational.com/drone-laws-by-country/mexico-drone-laws/.

[110] *Mexican Drone Regulations*, THE DRONE INFO (June 24, 2015), http://www.thedroneinfo.com/mexican-drone-regulations/.

operator or pilot must always keep the drone within his visual line of sight.[111] Finally, the regulations provide that all drones may not carry any dangerous merchandise or prohibited substances,[112] and pilots are responsible for any damage caused by an accident.[113]

As the foregoing discussion illustrates, Mexico's drone laws are not only new, but are not completely developed. That being said, commentators have stated that Mexico's drone laws are a step in the right direction, in part because they have closely modeled their regulations off of those currently in existence in the United States. However, both the drone regulations of Mexico and the United States are not fully comprehensive, leaving gaps for drones to be utilized in criminal activity, as displayed by the narcotics trafficking seen at the border.

IV. POSSIBLE SOLUTIONS TO PREVENT DRONES FROM BEING USED AS TOOLS FOR DRUG TRAFFICKING BY MEXICAN CARTELS

The previous sections have established the importance and impact of the use of drones to traffic narcotics into the United States. Factors contributing to the severity of this issue include the expanding drone industry, lack of drone regulations, and significant quantity of narcotics smuggled into the United States from Mexico. Based on the foregoing discussion, it is evident that the trafficking of narcotics from Mexico into the United States is nothing short of an epidemic. While certain drone regulations have been established by both Mexico and the United States, these regulations were not enacted to control the use of drones as tools for transporting narcotics. Since evidence suggests that Mexican cartels have begun to utilize drones as a trafficking technique, the need for a

---

111 CO AV-23/10 R2, art. 8, p. 5, available at http://www.sct.gob.mx /fileadmin/DireccionesGrales/DGAC/00-aeronautica/co-av-23-10-r2.pdf.

112 *Id.* at art. 7.2(e); see also *SCT announces new drone regulations*, MEXICO NEWS DAILY (Apr. 30, 2015), http://mexiconewsdaily.com/news/sct-announces-new-drone-regulations ("[drones] must not carry anything dangerous or illegal.").

113 CO AV-23/10 R2, art. 7.2(g), p. 4, available at http://www.sct.gob.mx/ fileadmin/DireccionesGrales/DGAC/00-aeronautica/co-av-23-10-r2.pdf.

comprehensive solution is imminent. This section proposes possible solutions to prevent drones from being used as tools by Mexican cartels for drug trafficking. This section will also discuss the regulation of drones in several other countries, and which policies, if any, should be adopted at the border.

It should be noted that while there exist several different theories to reduce the incidences of drug trafficking into the United States,[114] this comment focuses on methods that can be used to specifically prevent cartels from using drones to traffic narcotics. While alternative theories could undoubtedly decrease the overall incidences of narcotics trafficking into the United States, they will not be the focus of the discussion.

A. Overview of Proposal

The most important aspects of solving the drone crisis at the border are the FAA Modernization and Reform Act of 2012, the Merida Initiative, and the extradition treaty between the United States and Mexico. As discussed above, the FAA has been granted an extension to finalize their implementation of drones into the United States airspace.[115] The FAA should utilize the extension granted in the FAA Modernization and Reform Act to implement regulations for drone use at the border, and fill in any gaps not covered by the current regulations. The specifics of possible regulations will be discussed in subpart 1, below. These refined regulations within the FAA Modernization and Reform Act should then be implemented into collaborative drone regulations with the Mexican government at the border. This can be accomplished through the Merida Initiative, and specifically, through the first three pillars, which focus on disrupting organized criminal groups, strengthening institutions, and building a twenty-first century border. Such collaborative drone regulations would be consistent with the goals of the Merida

[114] *See inter alia* Mark Osler, SYMPOSIUM: DRUG POLICY REALITY AND REFORM: ASSET FORFEITURE IN A NEW MARKET-REALITY NARCOTICS POLICY, 52 Harv. J. on Legis. 221 (2015). (proposing that attacking the "cash flow" of the cartels would disrupt their narcotics operations).

[115] Aviation Pros, *supra* note 65.

Initiative. As part of the Initiative, the Mexican government must work to honor any new regulations implemented in the United States through the FAA Modernization and Reform Act. Finally, any criminal violations of the collaborative regulations would permit the United States to prosecute any offenders located in Mexico, due to the extradition treaty between the United States and Mexico. In order for this proposal to be effective, both countries must work to honor the treaty while respecting the other nation's sovereignty. With the basic framework of the proposal established, potential new drone regulations will be discussed below.[116]

1. *New Drone Regulations to be enacted through the FAA Modernization and Reform Act*.

To begin, both the United States and Mexico must enact regulations that explicitly ban the use of drones as drug trafficking tools at the border. No such regulation currently exists in either country, so this proposal is intuitively the first step in solving this problem. It is significant that a number of states have already enacted legislation prohibiting the weaponization of drones.[117] For this reason, a prohibition on the transportation of drugs would be feasible and consistent with existing drone regulations.

Next, the United States and Mexico should create harsher penalties for offenders who use drones to transport narcotics across the border. While trafficking narcotics across the border is already illegal,[118] a sentence enhancer for the use of drones would help deter future incidences of drone transportation, since the relatively small benefits of a single drone trafficking flight would not outweigh the potential enhanced sentence attached to such conduct. Such a sentence enhancer would also apply to those receiving the drone shipment within the United States. This proposal is closely related to

---

[116] While it is not anticipated that the cartels will follow every regulation this comment proposes, such regulations may nonetheless help deter cartels from using drones as trafficking tools by making the penalties for such conduct outweigh its potential benefits.

[117] *See inter alia* N.C. Gen. Stat. § 14-401.24 (2014).

[118] 21 USC § 841.

the first, however with slight differences. Whereas the previous proposal was an explicit ban on trafficking narcotics with drones, this proposal ensures a harsher penalty for those caught trafficking narcotics in this fashion. While the former is its own offense, the latter would attach to legislation already in existence.

Additionally, the United States and Mexico should categorize the region extending the length of the border as a "no fly zone" for drones, thus prohibiting unauthorized drone flights within 5 miles of the border.[119] This is accomplished by categorizing this region as "prohibited airspace," in which no drone operations may take place in a designated region of the border without the express permission of the United States or Mexican governments.[120] Any drone flights within this region, with the exception of drones currently controlled by the CBP,[121] would be strictly prohibited, and those participating in unauthorized flights would be subject to severe penalties as well as confiscation of any drone and narcotics being transferred across the border.[122] While such regions already exist, the border of the United States and Mexico is not included among these "no-fly zones."[123] As will be described below, several countries have adopted similar "no-fly zones" to help regulate drone flights.[124]

In conjunction with the prohibited airspace, all drone flights that fall outside of this region but nevertheless remain within 10 miles of the border must be operated within the line of sight of the operator – GPS and camera controlled flights should be strictly prohibited within this region. Adopting such a regulation would make it much more difficult for those attempting to traffic narcotics via

---

[119] Bobby Sudekum, *Don't fly drones here*, MAPBOX (July 22, 2014), https://www.mapbox.com/blog/dont-fly-here/ (Map of current no-fly zones for drones).

[120] 14 C.F.R.§§73.81-73.83 (2011).

[121] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, *supra* note 54.

[122] 21 U.S.C. § 881.

[123] FAA Modernization and Reform Act of 2012, Pub. L. 112-95, §334, 126 Stat. 11, 76-77.

[124] Canada prohibits flights within restricted airspace, including near or over military bases, prisons, and forest fires. *See* Canadian Aviation Regulations, SOR/96-433 (Can.) available at http://laws-lois.justice.gc.ca/PDF/SOR-96-433.pdf.

drones to remain hidden from authorities, and should make the risk of such a flight outweigh the potential benefits. This would also make drone trafficking flights less convenient, since they cannot be controlled through an automatic flight pattern with GPS coordinates or from a remote location via camera. To be effective, this regulation would also require the communities neighboring the border to be well informed of the regulation's requirements.

Finally, recall that the current United States and Mexican regulations categorize drones based on weight.[125] However with reports that the cartels are engineering their own drones with larger engines to make transporting narcotics more efficient,[126] regulations should be implemented prohibiting certain engine sizes for civilian drones. By limiting the engine size of drones that can be used for narcotics trafficking, such drones will be unable to carry greater weight, and thus will be unable to transport larger quantities of narcotics. Any drones seized that contain engine sizes exceeding the statutory limit will be subject to additional penalties. This regulation will help deter cartels from constructing their own drones with increased engine sizes, thus making drones an inefficient method for trafficking narcotics.

2. *Additional Methods.*

In addition to the above regulations, the United States and Mexico should employ the use of geo-fencing technology. Put simply, geo-fencing is a virtual barrier that surrounds a geographical boundary through the use of a GPS.[127] Geo-fencing technology could automatically prevent drones from entering a designated prohibited area. By designating the region extending the length of the border as

---

[125] FAA Modernization and Reform Act of 2012, Pub. L. 112-95, §336, 126 Stat. 11, 77-78; CO AV-23/10 R2, art. 7, p. 4, available at http://www.sct.gob.mx/fileadmin/DireccionesGrales/DGAC/00-aeronautica/co-av-23-10-r2.pdf.

[126] *Drug delivery drone crashes in Mexico*, BBC NEWS (Jan. 22, 2015), http://www.bbc.com/news/technology-30932395 (Stating that cartels hired engineers to manufacture drones to carry more weight than those that were commercially available.).

[127] *DEFINITION: geo-fencing (geofencing)*, TECHTARGET (Sep. 2015), http://whatis.techtarget.com/definition/geofencing.

prohibited airspace, as described above, the use of geo-fencing technology would ensure that GPS controlled drones do not fly within 10 miles of the border. This proposal is feasible, as U.S. lawmakers have recently suggested similar regulations.[128]

The United States must also continue utilizing their own surveillance drones at the border to help identify any unauthorized drones in the border airspace.[129] Since the drones utilized by the CBP already monitor the border for drug trafficking,[130] extending their operation to monitor the skies is the next logical and necessary step in preventing narcotics trafficking. In fact, China is currently utilizing drones in their own efforts to prevent drug trafficking on the Indian border in Tibet and in Xinjiang and Yunnan regions.[131] The use of such technology comes with its own weaknesses however, as drones utilized by the CBP may be susceptible to attacks.[132] Increased drone

---

[128] *See* Kim Kirschenbaum, *Recreational Drones Present Enforcement Issues for FAA*, UNIVERSITY OF PENNSYLVANIA LAW SCHOOL (Sept. 23, 2015), http://www.regblog.org/2015/09/23/kirschenbaum_recreational_drones/ (New York Senator Chuck Schumer recently announced his intentions to introduce an amendment mandating the use of geo-fencing technology on drones to restrict their flying capabilities.); *see also* Kaveh Waddell, *Chuck Schumer Wants to Set Up No-Drone Zones Around Airports*, NATIONAL JOURNAL (Aug. 19, 2015), http://www.nationaljournal.com/tech/2015/08/19/chuck-schumer-wants-set-up-no-drone-zones-around-airports (Geo-fencing technology proposals would create no-fly zones for "sensitive areas.").

[129] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, *supra* Note 54.

[130] *See* Thompson, *supra* note 17.

[131] *China deploys radars, drones on borders to curb infiltration*, THE ECONOMIC TIMES (Nov. 6, 2015), http://economictimes.indiatimes.com/news/defence/china-deploys-radars-drones-on-borders-to-curb-infiltration/articleshow/49688679.cms.

[132] *See* Scott Peterson & Payam Faramarzi, *Iran Hijacked US Drone, Says Iranian Engineer*, CHRISTIAN SCI. MONITOR (Dec. 15, 2011), http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video (Commentators have noted that the GPS guidance system that allows a UAS to fly free is highly susceptible to attack); *see also* Lorenzo Franceschi-Bicchierai, *Drone Hijacking? That's Just the Start of GPS Troubles*, WIRED (July 6, 2012), http://www.wired.com/dangerroom/2012/07/drone-hijacking/all/ ("There are already drones in use in the country that are plausible targets for jamming – think of the drones being used to monitor the border between the U.S. and Mexico for drug smuggling and border jumping.").

security could protect CBP drones from being hijacked,[133] and such techniques could then be used to ground unauthorized drones trafficking narcotics.[134]

B. Drone Regulations of Other Nations

Numerous countries around the world have enacted their own unique drone regulations, the adoption of which may be useful to the United States and Mexico in their efforts to combat narcotics trafficking. The following discussion explores a number of drone regulations from several countries. While some of the outlined regulations may prove to be useful in the future of drone regulation at the border, others are included to provide a simple comparison. This discussion is intended to highlight how the regulations of Mexico and the United States compare to those of other nations, and discuss which regulations may be useful to help curb the incidences of drones being used to traffic narcotics across the border. The countries described below were selected based on a unique feature about their drone regulations, and provided a distinct basis of comparison to the drone regulations of Mexico and the United States.

1. *United Kingdom.*

To begin, drone regulations in the United Kingdom are very similar to those of the United States. One notable difference is that the United Kingdom requires direct visual contact to be maintained at all times, and the operator may not use a monitor to conduct the

---

[133] Bellow, *supra* note 86 at 615 ("The FAA should also require that all UASs come equipped with some sort of anti-drone-jacking technology.").

[134] Josh Solomon, Unc*ertainties Remain as FAA Integrates Drones Into American Skies*, MCCLATCHY DC (April 29, 2013), http://www.mcclatchydc.com/2013/04/29/189894/uncertainties-remain-as-faa-integrates.html ("Drones also are susceptible to communications jamming, leaving the operator unable to control the aircraft.").

flight.[135] A similar regulation should be enforced at the designated 10-mile zone at the border, discussed above. This would prohibit GPS or camera operated flights, thus forcing pilots to keep the drone in their line of sight. In turn, this UK regulation would increase the risk that a potential trafficker will be identified.

2. *Canada.*

As previously noted, Canada prohibits flights within restricted airspace, including near or over military bases, prisons, and forest fires.[136] A similar regulation could create a "no-fly zone" within five miles of the border, and impose severe fines or penalties for any violators caught operating an unauthorized drone in this region. Additionally, Canada prohibits operating a drone in a region that would interfere with first responders.[137] A similar regulation could be implemented at the border, prohibiting drone flights that could interfere with drones currently being utilized by the CBP.

3. *Bangladesh.*

Contrary to the United States and Mexico, the Government of Bangladesh has banned all drones that did not have flight permission prior to December 2014.[138] While an interesting approach to drone regulation, a similar approach would likely be far too drastic in the United States and Mexico, where demand for drones are skyrocketing, and would not directly solve the issue of drones used as trafficking tools. Nevertheless, the approach to drone regulations in Bangladesh is an interesting contrast to the regulations discussed in the United States and Mexico.

---

[135] *Above the Law: How Drone Laws Around the World Are Affecting Production*, LITTLE BLACK BOOK LTD. (Sept. 2014), http://www.lbbonline.com/news/above-the-law-how-drone-laws-around-the-world-are-affecting-production/.

[136] *See* Canadian Aviation Regulations, *supra* note 124.

[137] *Id.*

[138] *No drone allowed in country's airspace*, THE DAILY STAR (Dec. 31, 2014), http://www.thedailystar.net/no-drone-allowed-in-countrys-airspace-57769; *see also* CIVIL AVIATION AUTHORITY, BANGLADESH, http://www.caab.gov.bd (last visited Jan. 7, 2016).

4. *Brazil.*

On the opposite end of the spectrum, Brazil does not have any restrictions on drone usage within their country.[139] The country intended to implement new drone legislation before the 2016 Olympics,[140] however such measures were largely unsuccessful.[141] While not a practical solution by any means, this *laissez faire* approach to drone regulation is interesting in the context of the rising drone market across the globe.

5. *Austria.*

Austria requires that potential drone users either have a pilot license or pass an exam about Austrian air law.[142] While such a regulation may seem harsh, it undoubtedly would increase the security of the border, permitting only trained pilots or those with requisite knowledge to pilot drones. While such a regulation may not directly have any deterring effects on the trafficking of narcotics into the United States via drones, this regulation would increase the safety of the communities at the border by enhancing notice of the no-fly zones and applicable drone laws prohibiting trafficking.

6. *The Netherlands.*

The final, and most outlandish, method of drone regulation in a foreign country is found in the Netherlands. While not exactly a regulation, it is worth mentioning that the Dutch National Police

---

[139] *Above the Law: How Drone Laws Around the World Are Affecting Production*, LITTLE BLACK BOOK LTD. (Sept. 2014), http://www.lbbonline.com/news/above-the-law-how-drone-laws-around-the-world-are-affecting-production/.

[140] *Brazil to Unveil New Drone Legislation ahead of 2016 Olympics*, PANAM POST (Apr. 17, 2015), https://panampost.com/panam-staff/2015/04/17/brazil-to-unveil-new-drone-legislation-ahead-of-2016-olympics/.

[141] Russell Brandom, *How Brazil is trying (and failing) to keep drones away from the Olympics*, THE VERGE (Aug. 8, 2016), http://www.theverge.com/2016/8/8/12402972/olympics-rio-2016-anti-drone-jamming-public-safety.

[142] BUNDES-VERFASSUNGSGESETZ [B-VG] [CONSTITUTION] BGBl No. 253/1957, as amended by Bundesgesetz [BGBl] No. 96/2013, art. 4, § 24 (Austria).

Corps has begun a new initiative using eagles to capture unauthorized drones from the sky.[143] The eagle responds to the drone as it would its normal prey, snatching the drone mid-flight and carrying it to the ground. It has been explained that "these birds' animal instincts . . . offer an effective solution to a new threat."[144] While this technique may seem impractical, one cannot deny the poetic justice of seeing a bald eagle protect the American border by snatching a shipment of illicit narcotics from the sky.

V. CONCLUSION

The use of drones to traffic narcotics into the United States from Mexico is an increasing phenomenon that is contributing to the United States' drug epidemic. Drones are becoming more widely available, and the current regulations cannot keep up with this expansion. The need for a solution is imminent as we move into 2017. The current drone regulations of Mexico and the United States are insufficient to solve this crisis, however the pieces of a solution have been put into place. The United States needs to utilize the recent extension of the FAA Modernization and Reform Act to ensure that new regulations are enacted to help prevent future incidences of drug trafficking into the United States. Potential regulations include explicit bans on using drones as trafficking tools as well as sentence enhancers for such uses, categorizing the border as prohibited airspace or a "no-fly zone," and limitations on drone engine sizes. These regulations could be promulgated through the FAA Modernization and Reform Act, and implemented into Mexico's own drone legislation through the Merida Initiative. Once these two nations have collaborative drone regulations at the border, they should continue to honor the extradition treaty they signed in 1978. In addition to the above framework, both countries should utilize geo-fencing technology, thus creating virtual barriers for any GPS piloted flights. The United States CBP should continue using

---

143 Mindy Weisberger, *Drone-hunting eagles can snatch devices out of the sky*, CBS NEWS (Feb. 8, 2016), http://www.cbsnews.com/news/drone-hunting-eagles-can-snatch-the-devices-out-of-the-sky/.

144 *Id.*

their own drones at the border to not only identify potential traffickers on foot, but to monitor the skies for any unauthorized drones. It is important that the CBP ensure these drones are equipped with anti-drone-jacking technology, and should not hesitate to use such technology to ground unauthorized drones. Finally, various regulations (or lack thereof) from the United Kingdom, Canada, Bangladesh, Brazil, Austria, and the Netherlands provide a unique dialogue on regulations that the United States and Mexico could potentially implement at the border.

While drones may not currently be the primary method for Mexican cartels to traffic narcotics into the United States, this reality could change if the United States and Mexico do not take steps to prevent its continued use in the future. The use of drones at the border has implications beyond drug trafficking,[145] however their use as trafficking tools can no longer be ignored. With an extension granted to the FAA for the promulgation of new regulations, only time will tell if this new drug trafficking method can be grounded before it finally takes off.

[145] *See* Bellow, *supra* note 86, at 609 ("[T]hose with nefarious purposes could turn large-scale UASs into projectile weapons against the American people or attempt to weaponize UASs and open fire on the public.").

Penn State
Journal of Law & International Affairs

2017 VOLUME 5 NO. 1

ADRIFT AT SEA: HOW THE UNITED STATES GOVERNMENT IS FORGOING THE FOURTH AMENDMENT IN THE PROSECUTION OF CAPTURED TERRORISTS.

Frank Sullivan

TABLE OF CONTENTS

I. INTRODUCTION

Since September 11th, 2001, the United States Government has faced the ever-evolving challenge of combating foreign terrorists. The capture of a suspected terrorist by United States forces presents several legal issues, including, questions over the nature of the terrorism suspect's capture, subsequent treatment and afforded rights.[1]

Additionally, United States Government officials face the controversial decision about what to do with captured terrorism suspects: either detain them as enemy combatants at Guantanamo Bay to face a military tribunal, or try them before a civilian court in the United States.[2] Since the attacks of September 11th and the beginning of the War on Terror, terrorism suspects have been tried in military tribunals as well as civilian courts. However, under the current administration, the preferred method has been to seek justice in civilian courts.[3]

Recently, suspected ringleader of the 2012 Benghazi terrorist attack,[4] Ahmed Abu Khatallah,[5] has been subjected to this policy, and

---

[1] *See* Steve Vladeck, *Kidnapping Is Legally Dubious, But It's Also The Best Way To Get Terrorists*, WASH. POST, June 18, 2014 (presenting legal issues regarding rendition of terrorist suspects).

[2] For arguments promoting both sides in one particular case, see Karen DeYoung, Adam Goldman and Julie Tate, *U.S. Captures Benghazi Suspect In Secret Raid,* WASH. POST, June 17, 2014.

[3] *See* Karen DeYoung, Adam Goldman and Julie Tate, *U.S. Captures Benghazi Suspect In Secret Raid,* WASH. POST, June 17, 2014.

[4] For more information on the Benghazi attack, including background on Ahmed Abu Khatallah as well as details of the attack from several witnesses close to Abu Khatallah and present on the night of the attack, see David D. Kirkpatrick, *A Deadly Mix In Benghazi*, N.Y. TIMES, Dec. 28, 2013, http://www.nytimes.com/projects/2013/benghazi.

[5] While the English spelling of his name sometimes differs based on the source, from 'Khattala' to 'Khatallah,' this comment uses the spelling 'Khatallah,' which is used in the formal Indictment filed by the United States Attorney's Office for the District of Columbia. *See* Indictment at 1, United States v. Abu Khatallah, No.14-141 (2014).

is being tried in a civilian court in Washington D.C.[6] Charged in relation to the September 11th, 2012, attack on the United States diplomatic compound in Benghazi, Libya, in which Ambassador J. Christopher Stevens, Foreign Service Information Management Officer Sean Patrick Smith, and CIA Security Officers Tyrone Snowden Woods and Glen Anthony Doherty were killed,[7] suspected leader of Ansar al-Sharia, Ahmed Abu Khatallah, was captured by a team of United States Special Forces in mid-June, 2014.[8] After his capture in Libya, Ahmed Abu Khatallah was immediately transported to an American military vessel, the *USS New York*, which transported Khatallah across the Atlantic Ocean to face trial in federal court in the District of Columbia.[9]

The capture and subsequent handling of Ahmed Abu Khatallah implicates several legal questions surrounding United States policy regarding the capture of suspected terrorists.[10] Despite questions surrounding the handling of Abu Khatallah, the decision by the Obama administration to transport Abu Khatallah back to the United States on an American military ship was both deliberate and strategic.[11] By choosing to transport Abu Khatallah by military ship,[12]

---

[6] *See* Karen DeYoung and Ann E. Marimow, *Benghazi Suspect Ahmed Abu Khattala May Be Brought To U.S. On Navy Ship,* WASH. POST, June 18, 2014.

[7] *See* Government's Motion For Pretrial Detention at 7, United States v. Abu Khatallah, No.14-141 (2014).

[8] *See Id.* at 10.

[9] *See* Thomas Gibbons-Neff, *USS New York, Carrying a Benghazi Suspect, Has Gone Dark,* WASH. POST, June 25, 2014.

[10] *See* Ben Brumfield, *What's Next For Benghazi Terror Suspect Ahmed Abu Khatallah?,* CNN, June 18, 2014.

[11] The reasoning for doing so primarily revolves around the rather dubious nature of the capture of the suspect by extraordinary rendition. The difficulty in finding countries willing to allow suspects who have been subject to rendition to pass through their sovereign territory during the process of transporting the suspect to America makes transportation by way of military ship extremely convenient, if not necessary. *See* Ben Brumfield, *What's Next For Benghazi Terror Suspect Ahmed Abu Khatallah?,* CNN, June 18, 2014.

[12] Whether the United States is legally able to use the military for purposes of law enforcement is a separate, distinct legal question. Under the Posse Comitatus Act, the armed forces are restrained from aiding civilian law enforcement authorities in keeping the peace and arresting felons. *See* 18 U.S.C. § 1385 (1978). *See also* 10 U.S.C. § 375 (1981) (requiring the Department of Defense to prescribe

the Obama administration had several days to question and search Abu Khatallah before the vessel reached the United States.[13] Further, because much of the trip from Libya to the United States involved crossing the Atlantic Ocean, in international waters, FBI agents were able to search Abu Khatallah without a warrant and question him without reading him his Miranda rights.[14]

This article will argue that the current Administration's practice of searching individuals without a warrant by way of transporting suspected terrorists[15] on military ships through international waters is in direct conflict with the Fourth[16] Amendment.[17] On its face, this practice appears to comply with

---

regulations ensuring that the U.S. Navy, among others, does not directly participate in civilian law enforcement absent authorization by law). The Department of Justice maintains the Posse Comitatus Act does not apply outside of the territory of the United States, and as such, for the purposes of this article, it will be assumed that the United States Government's practice of using military vessels in a law enforcement capacity for suspects bound for civilian courts is itself legal. *See* Int'l Law Dep't, U.S. Naval War College, U.S. Navy, NWP 1-14M, The Commanders Handbook on the Law of Naval Operations, § 3.11.3.1, p. 3-13 (2007).

[13] *See* Evan Perez and Holly Yan, *Controversy Swirls Over Handling Of Benghazi Suspect Abu Khatallah,* CNN, June 29, 2014 (Ahmed Abu Khatallah questioned aboard ship for two weeks).

[14] *See* Michael Schmidt, Matt Apuzzo, Eric Schmitt and Charlie Savage, *Trial Secondary As U.S. Questions a Libyan Suspect,* N.Y. TIMES, June 19, 2014.

[15] Ahmed Abu Khatallah is not the first suspected terrorist held aboard military vessels pending transfer to the United States. *See* Charlie Savage, *U.S. Tests New Approach to Terrorism Cases on Somali Suspect*, N.Y. TIMES, July 6, 2011 (describing the handling of Somali Ahmed Abdulkadir Warsame aboard the *USS Boxer*); Benjamin Weiser and Eric Schmitt, *U.S. Said to Hold Qaeda Suspect on Navy Ship*, N.Y. TIMES, Oct. 6, 2013 (Libyan Abu Anas al-Libi aboard the *USS San Antonio*).

[16] The Fourth Amendment reads: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

[17] Again, recognizing that contravention of the Fourth Amendment is likely only a collateral benefit and not the official reasoning for the use of military ships to transport suspected terrorists, *see* Note 11 *supra*. Additionally, this discussion will be limited to the applicability of the Fourth Amendment to Abu Khatallah, as well as similarly situated suspected terrorists. Questions surrounding Miranda and the Public Safety Exception, while extremely important and relevant to Abu Khatallah,

numerous Supreme Court cases establishing the extraterritorial reach of the Fourth Amendment.[18] However, the Supreme Court's decision in *Boumediene v. Bush*[19] raises questions regarding the applicability of the Fourth Amendment on a United States military vessel, even if the ship is located in international waters.

To answer these questions, it is necessary to first understand the extraterritorial applicability of the Constitution. Part II of this article will describe the extraterritoriality of the United States Constitution. Part III will explore the Supreme Court's ruling in *Boumediene* and its impact on the extraterritorial application of the Constitution. Part IV will examine the United States' position on the jurisdiction surrounding American military vessels. Part V discusses a few policy considerations implicated by the analysis of Parts II-IV.

II. THE EXTRATERRITORIALITY OF THE CONSTITUTION

The extraterritoriality of the Constitution can be broken down as it applies to three main categories of individuals: (1) non-United States citizens present within the territory of the United States, (2) United States citizens outside of the territory of the United States, and (3) non-United States citizens outside of the territory of the United States.

Section A will give a brief overview of the applicability of the Constitution to the first two categories, non-United States citizens within the United States and United States citizens abroad. Section B will give a more in-depth look at the category in which Ahmed Abu

---

as well as other similarly situated suspected terrorists, are too much to address here and will be saved for another time.

[18] *See* United States v. Verdugo-Urquidez, 494 U.S. 259 (1990) (Fourth Amendment does not apply to foreign citizens in foreign territories); INS V. Lopez-Mendoza, 468 U.S. 1032 (1984) (assuming illegal aliens in the United States have Fourth Amendment rights); Reid v. Covert, 354 U.S. 1 (1957) (Constitutional provisions applicable to United States citizens abroad); Johnson v. Eisentrager, 339 U.S. 763 (1950) (no extraterritorial application of the Fifth Amendment).

[19] 553 U.S. 723 (2008).

Khatallah falls, a non-United States citizen located outside of the United States.

A. Applicability to non-United States Citizens within the United States, and United States Citizens Abroad.

In *Kwong Hai Chew v. Colding*,[20] the Supreme Court addressed the issue of whether a Chinese national lawfully living in the United States could be detained without first receiving notice of the charges levied against him, while further denying the individual any opportunity to voice their opposition to the detention.[21] The Supreme Court held that non-United States citizens present within the United States are afforded constitutional protections.[22] In deciding the case, the Court stated the "well-established" principle that, if an alien is lawfully present in the United States, he is within the protection of the Fifth Amendment and may not be deprived of life, liberty or property without due process.[23]

The Supreme Court first addressed whether the Constitution, and more specifically the Fifth and Sixth Amendments, apply to United States citizens outside of the United States in *Reid v. Covert.*[24] In *Reid*, the Court addressed the issue of whether military trials of civilian spouses of servicemen stationed abroad were constitutional.[25] Upon rehearing and reconsideration, the Supreme Court reversed their earlier decision[26] and held that civilian spouses of servicemen

[20] 344 U.S. 590 (1953).

[21] *Kwong Hai Chew*, 344 U.S. at 595.

[22] *Id.* at 600.

[23] *Id.* at 596. *See also* Bridges v. Wixon, 326 U.S. 135, 161 (1945) (Murphy, J., concurring) ("Once an alien lawfully enters and resides in this country he becomes invested with the rights guaranteed by the Constitution to all people within our borders.); Johnson v. Eisentrager, 339 U.S. 763, 770-771 (1950) (Mere lawful presence in the country creates an implied assurance of safe conduct and gives him certain rights.).

[24] 354 U.S. 1 (1957).

[25] *Reid*, 354 U.S. at 5.

[26] *See* Kinsella v. Krueger, 351 U.S. 470, 487 (1956) (holding that Fifth and Sixth Amendments do not protect American citizens tried by the American Government for crimes committed and tried in a foreign land).

stationed abroad could not be tried by a military tribunal.[27] Trying a civilian in a military tribunal was held to be in violation of the civilian's Fifth[28] and Sixth[29] Amendment rights.[30]

The Supreme Court reasoned that, because the United States' power and authority is solely created by the Constitution, the Government must act within constitutional limitations.[31] The Court rejected the argument that only fundamental constitutional rights protect Americans abroad.[32] Instead, the Court found in favor of extending every provision of the Constitution to American citizens, either at home or in another land.[33]

Kwong Hai Chew and *Reid* thus begin to define the breadth and limits of constitutional applicability. Instead of universal applicability, the Constitution applies to United States citizens, in the United States as well as abroad, and to foreign nationals that are lawfully within the territory of the United States. However, one question remains: do the provisions of the Constitution restrain the United States when it acts against a foreign national outside of the territory of the United

---

[27] *Reid*, 354 U.S. at 5.

[28] The Fifth Amendment reads, in pertinent part: "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger... nor be deprived of life, liberty, or property, without due process of law." U.S. Const. amend. V.

[29] The Sixth Amendment reads, in pertinent part: "In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed." U.S. Const. amend. VI.

[30] *Reid*, 354 U.S. at 5.

[31] *Id.* at 6 (citing Marbury v. Madison, 1 Cranch 137, 176-180 (1803)).

[32] *Reid*, 354 U.S. at 9.

[33] *Id.* at 9. However, courts have since limited the extent to which some constitutional provisions apply to citizens outside of the United States. *See e.g.,* In re Terrorist Bombings of U.S. Embassies in East Africa (Fourth Amendment Challenges), 552 F.3d 157, 167 (2nd Cir. 2008) (holding that "the Fourth Amendment's warrant requirement does not govern searches conducted abroad by U.S. agents; such searches of U.S. citizens need only satisfy the Fourth Amendment's requirement of reasonableness.").

States? The Supreme Court first addressed this question in *United States v. Verdugo-Urquidez*.[34]

B. Applicability to non-United States Citizens Outside the United States.

For decades, the Supreme Court's landmark decision in *Verdugo* has stood as the guidepost for determining whether foreign citizens located outside of the United States have rights under the United States Constitution. In *Verdugo,* the Supreme Court addressed whether the Fourth Amendment's warrant requirement was violated when Drug Enforcement Agency (DEA) agents searched the defendant's house without a search warrant.[35] The Court ultimately held that because the defendant was a Mexican national, and the property searched was located in Mexico, the Fourth Amendment did not apply.[36]

The defendant in *Verdugo,* a citizen and resident of Mexico, was apprehended by Mexican authorities based on an American arrest warrant issued in connection with narcotics distribution.[37] The Mexican citizen was transported to the Mexican-American border where he was delivered to United States Marshals for arrest.[38] Following the arrest, DEA agents, in conjunction with Mexican Federal Judicial Police Officers searched the defendant's properties in Mexicali and San Felipe and seized evidence of the defendant's narcotics trafficking.[39]

At trial, the District Court for the Southern District of California suppressed the seized evidence, concluding that the Fourth Amendment applied to the search and that there had been no justification for searching the premises without a warrant.[40] The

[34] 494 U.S. 259 (1990).
[35] *Verdugo,* 494 U.S. at 261.
[36] *Id.* at 274-75.
[37] *Id.* at 262.
[38] *Id.*
[39] *Verdugo,* 494 U.S. at 262.
[40] *Id.* at 263.

Court of Appeals for the Ninth Circuit, although divided, affirmed the District Court's ruling by relying on *Reid*.[41] On further appeal, in a 6-3 decision, the Supreme Court held that the Fourth Amendment did not apply to the defendant because at the time of the search, the defendant "was a citizen and resident of Mexico with no voluntary attachment to the United States, and the place searched was located in Mexico."[42]

Chief Justice Rehnquist, writing for the majority opinion, examined the function of the Fourth Amendment compared to the Fifth Amendment, which was at issue in *Reid*.[43] Chief Justice Rehnquist stated that while constitutional violations of the Fifth Amendment occur at trial, violations of the Fourth Amendment are "fully accomplished" at the time of the search.[44] Therefore, even if there was a constitutional violation of the defendant's Fourth Amendment rights, it occurred solely in Mexico.[45] Remedial exclusion of the evidence is a separate question and does not touch on the existence of a constitutional violation in and of itself.[46]

The Chief Justice, in an effort to determine whether the Fourth Amendment was meant to apply to foreign nationals, analyzed the language and history of the Fourth Amendment.[47] First, the language of the Fourth Amendment, using the term of art 'the people,' refers to "a class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community."[48]

Second, the history of the Fourth Amendment suggests that its provisions were meant to protect the American people against arbitrary action by the United States Government, and not intended to restrain the actions of the United States Government against aliens

---

41 *Id.*
42 *Id.* at 274-75.
43 *Id.* at 264.
44 *Id.*
45 *Verdugo*, 494 U.S. at 264.
46 *Id.*
47 *Id.* at 265.
48 *Id.*

outside American territory.[49] As an example, Chief Justice Rehnquist noted that in 1798 Congress passed an act allowing commanders of both public and private armed vessels of the United States to "subdue, seize and take any armed French vessel . . . on the high seas."[50] While some commanders were held liable for seizures beyond the scope of Congress' grant of authority,[51] the Supreme Court never suggested the Fourth Amendment restrained commanders from conducting such seizures authorized by Congress.[52]

Finally, Chief Justice Rehnquist looked at previous case law to determine whether the Fourth Amendment applied to the DEA search conducted in Mexico.[53] The opinion in *Verdugo* stated that the Court of Appeals' global application of the Constitution goes against precedential cases, known as the *Insular Cases*.[54] As Chief Justice Rehnquist points out, the *Insular Cases*[55] held that not every constitutional provision applies to Government activity, even when the United States may have sovereign power, and that only fundamental constitutional rights are guaranteed to inhabitants of unincorporated territories of the United States.[56] Because the Constitution "does not, without legislation and of its own force" apply to territories ultimately governed by Congress, the claim that

---

[49] *Id.* at 266.

[50] *Id.* at 267. *See also* §§ 1-2 of An Act Further to Protect the Commerce of the United States, ch. 68, 1 Stat. 578-9.

[51] *See, e.g.*, Little v. Barreme, 2 Cranch 170, 177-178 (1804); *cf.* Talbot v. Seeman, 1 Cranch 1, 31 (1801) (seizure of neutral ship lawful where American captain had probable cause to believe vessel was French).

[52] *Verdugo,* 494 U.S. at 268.

[53] *Id.*

[54] *Id.*

[55] *See, e.g.,* Balzac v. Porto Rico, 258 U.S. 298 (1922) (Sixth Amendment right to jury trial inapplicable in Puerto Rico); Ocampo v. United States, 234 U.S. 91 (1914) (Fifth Amendment grand jury provision inapplicable in Philippines); Dorr v. United States, 195 U.S. 138 (1904) (jury trial provision inapplicable in Philippines); Hawaii v. Mankichi, 190 U.S. 197 (1903) (jury trial and indictment by grand jury provisions inapplicable in Hawaii); Downes v. Bidwell, 182 U.S. 244 (1901) (Revenue Clauses inapplicable to Puerto Rico).

[56] *Verdugo,* 494 U.S. at 268 (citing *Dorr,* 195 U.S. at 148).

protections of the Fourth Amendment extend to aliens in foreign nations is especially weak.[57]

In addition to the *Insular Cases*, Chief Justice Rehnquist found support for holding that the Fourth Amendment does not apply to foreign nationals in foreign territories in *Johnson v. Eisentrager*.[58] The Chief Justice emphasized that while some constitutional provisions extend beyond the citizenry of the United States, the *Eisentrager* opinion emphatically rejected the extraterritorial application of the Fifth Amendment, as the extraterritorial application of organic law is a practice that every modern government is opposed to.[59]

In contrast to the *Insular Cases* and *Eisentrager,* the Chief Justice distinguished *Verdugo* from the *Reid* decision relied on by the lower courts.[60] In quoting from the *Reid* decision, Chief Justice Rehnquist emphasized that, "when the government reaches out to punish *a citizen* who is abroad, the shield which the Bill of Rights and other parts of the Constitution provided to protect his life and liberty should not be stripped away just because he happens to be in another land."[61] While the lower courts interpreted such language as constraining federal officials under the Fourth Amendment wherever and against whomever they act, the Chief Justice stated that *Reid* dealt with United States citizens abroad and that the holding of *Reid* is therefore not applicable to the case at hand.[62]

Chief Justice Rehnquist similarly rejected the contention that case law dealing with the application of the Constitution to foreign nationals within the United States[63] applies to the case at hand because the defendant in *Verdugo* had no voluntary connection with the United States, and foreign nationals can only avail themselves of

---

[57] *Verdugo,* 494 U.S. at 268 (citing *Dorr,* 195 U.S. at 149).

[58] 339 U.S. 763 (1950) (rejecting the claim that enemy aliens imprisoned in Germany after World War II are entitled to habeas corpus writs in federal courts on the ground that their war crimes convictions were violations of the Fifth Amendment and other constitutional provisions).

[59] *Verdugo,* 494 U.S. at 269 (citing *Eisentrager,* 339 U.S. at 784).

[60] *Verdugo,* 494 U.S. at 270.

[61] *Verdugo,* 494 U.S. at 270 (quoting *Reid*, 354 U.S. at 5-6).

[62] *Verdugo,* 494 U.S. at 270.

[63] *See Kwong Hai Chew*, *supra* note 21.

the protections of the Constitution when they come within the territory of, and develop substantial connections with, the United States.[64] In response to Justice Stevens' concurrence,[65] Chief Justice Rehnquist stated that the applicability of the Fourth Amendment should not turn on the "fortuitous circumstance" that the foreign national had been transported to the United States prior to the search. Chief Justice Rehnquist maintained that only voluntary presence in the United States invokes constitutional protections for foreign nationals.[66]

In his concurrence, Justice Kennedy noted that in addition to the reasoning of the Chief Justice, practicality concerns also weigh in favor of the Fourth Amendment not having any application to searches of foreign nationals in foreign territories.[67] Justice Kennedy reasoned that due to the absence of local magistrates or judges in foreign territories that have the authority or ability to issue American search warrants, as well as the "differing and perhaps unascertainable conceptions of reasonableness" in foreign territories, the warrant requirement of the Fourth Amendment should not apply in foreign territories as it does in the United States.[68] Likewise, Justice Stevens concurred with the majority opinion that the Fourth Amendment does not apply, primarily because American magistrates have no authority to authorize searches in foreign territories.[69]

---

[64] *Verdugo,* 494 U.S. at 271. (citing Plyer v. Doe, 457 U.S. 202, 212 (1982) ("The provisions of the Fourteenth Amendment are universal in their application, *to all persons within the territorial jurisdiction*…") (emphasis in original); *Kwong Hai Chew*, 344 U.S. at 596("But *once an alien lawfully enters and resides in this country* he becomes invested with the rights guaranteed by the Constitution to all people within our borders") (emphasis in original)).

[65] In his concurrence, Justice Stevens stated that aliens lawfully present in the United States are protected by the Fourth Amendment, regardless of whether they are present voluntarily or, as in the case at hand, involuntarily. *Verdugo,* 494 U.S. at 279 (Stevens, J., concurring).

[66] *Verdugo*, 494 U.S. at 272. However, the voluntary presence standard failed to gain acceptance by a majority of the Court and is therefore dicta.

[67] *Verdugo,* 494 U.S. at 278 (Kennedy, J., concurring).

[68] *Id.* Additionally, in his dissent, Justice Blackmun agreed that the Warrant Clause does not apply and searches conducted abroad are subject only to the reasonable aspect of the Fourth Amendment. *Id.* at 297 (Blackmun, J., dissenting).

[69] *Verdugo*, 494 U.S. at 279 (Stevens, J., concurring).

Applying the Supreme Court's previous analyses of the scope of the Constitution to the Government's actions in dealing with Ahmed Abu Khatallah, it seems that the Constitutional protections of the Fourth Amendment do not apply. First, Abu Khatallah is not a citizen of the United States, and therefore cannot avail himself of the Fourth Amendment's protections on the grounds of citizenship. Second, the search of Abu Khatallah did not occur in the territory of the United States, but rather occurred in international waters, eliminating the protections of the Fourth Amendment afforded non-citizens within the United States. Lastly, while an argument can be made that Abu Khatallah was in the possession of the United States when he was searched, the Chief Justice's "voluntary connection" language from *Verdugo* suggests that because Abu Khatallah had no connection to the United States other than his capture and subsequent rendition to justice, which is most certainly not a voluntary connection, the Fourth Amendment does not apply.

Following the *Verdugo* holding, the United States could have viably searched, without a search warrant, not only Abu Khatallah's physical person in international waters, but also any properties owned by Abu Khatallah outside of the United States (i.e., his house in Libya). However, the Supreme Court's decision in *Boumediene v. Bush* raises questions as to whether the Constitution in fact does apply to Abu Khattallah, and whether the Government's search of Abu Khatallah was legal.

III. *BOUMEDIENE V. BUSH* AND *DE FACTO* JURISDICTION THROUGH EXCLUSIVE CONTROL

In *Boumediene,* the Supreme Court dealt with several issues revolving around foreign national enemy combatants held at Guantanamo Bay.[70] Specifically, the Supreme Court addressed whether foreign nationals detained at Guantanamo Bay could avail themselves of the constitutional protection of the Writ of Habeas

[70] *Boumediene*, 553 U.S. at 732.

Corpus.[71] The Supreme Court in *Boumediene* denied the Government's argument that the foreign nationals were held in territory outside of the Nation's borders, which therefore leaves the detainees without constitutional rights,[72] and concluded that foreign nationals detained as enemy combatants at Guantanamo Bay may invoke the protections of habeas corpus.[73] In doing so, the Supreme Court created a functional test to determine the extraterritorial reach of the Constitution.[74]

Writing for the majority, Justice Kennedy acknowledged that pursuant to the agreement between Cuba and the United States, Cuba retains "ultimate sovereignty," while the United States exercises "complete jurisdiction and control" over Guantanamo Bay.[75] Because of this division of power, Justice Kennedy stressed that while Cuba has *de jure* jurisdiction over Guantanamo Bay, the United States nonetheless has *de facto* jurisdiction.[76] This distinction ultimately lead Justice Kennedy to conclude that "[i]n every practical sense Guantanamo [Bay] is not abroad; it is within the constant jurisdiction of the United States."[77] Because of the "complete and total control" of the United States over Guantanamo Bay, foreign detainees held there could avail themselves of the constitutional protections of habeas corpus.[78]

Justice Kennedy found support for the holding in the lack of prudential concerns previously preventing the extension of habeas corpus to territories under the sovereign control of a different nation.[79] Specifically, Justice Kennedy noted that there was no reason

---

[71] *Id.*

[72] *Id.* at 739.

[73] *Id.* at 798.

[74] *Id.* at 764.

[75] *Boumediene*, 553 U.S. at 753. *See also* Lease of Lands for Coaling and Naval Stations, Feb. 23, 1903, U.S.-Cuba, Art. III, T.S. No. 418.

[76] *Boumediene*, 553 U.S. at 755.

[77] *Id.* at 769.

[78] *Id.* at 771.

[79] *Boumediene,* 553 U.S. at 751. *See generally* King v. Cowle, 2 Burr. 834 (As a territory that was not a part of England, yet controlled by the English monarch, the writ of habeas corpus was never extended to Scotland); R. Sharpe, The Law of Habeas Corpus 191 (2d ed. 1989). *See also* Note on the Power of English Courts to

to believe that a federal court's order would be disobeyed at Guantanamo Bay, and that no other law besides that of the United States applies to the naval base.[80]

Additionally, Justice Kennedy attempted to reconcile his functional holding with previous case law. First, in addressing the *Insular cases*, Justice Kennedy found that by utilizing the doctrine of territorial incorporation,[81] the Court devised a functional approach to the application of the Constitution.[82] This approach served as a foundation to the functional approach established by the Supreme Court in *Boumediene*.[83]

Second, Justice Kennedy found support for his holding in the practical concerns that influenced the Court in *Reid*.[84] Justice Kennedy read *Reid* to rely not on the citizenship of the petitioners, but instead on the petitioner's place of confinement and trial.[85] Relying primarily on Justice Frankfurter's and Justice Harlan's concurrences in *Reid*, Justice Kennedy noted that *Reid* rejected a rigid rule in favor of analyzing the circumstances of each particular case when applying the Constitution extraterritorially.[86]

Issue the Writ of Habeas to Places Within the Dominions of the Crown, But Out of England, and On the Position of Scotland in Relation to that Power, 8 Jurid. Rev. 158 (1896).

[80] *Boumediene*, 553 U.S. at 751.

[81] Under the doctrine of territorial incorporation, utilized in the *Insular cases*, the Constitution is fully incorporated and applies only to territories destined for statehood. For unincorporated territories (those not destined for statehood) the Constitution only applies in part, determined by the situation of the territory and its relationship to the United States. *See Dorr*, 195 U.S. at 143.

[82] *Boumediene*, 553 U.S. at 759. *See also Balzac*, 258 U.S. at 312.

[83] *Boumediene*, 553 U.S. at 764.

[84] *Id.* at 759.

[85] *Id.* at 760.

[86] *Boumediene*, 553 U.S. at 768. In his concurrence to *Reid* Justice Harlan rejected a "rigid and abstract rule," reading the *Insular cases* to mean that constitutional provisions' extraterritorial effect depends on the particular circumstances, particularly whether judicial enforcement would be "impracticable and anomalous." *Reid*, 351 U.S. at 74-75 (Harlan, J., concurring in result). *See also Reid*, 351 U.S. at 54 (Frankfurter, J., concurring in result).

Lastly, to reconcile his holding with the holding of *Eisentrager*, Justice Kennedy distinguished Landsberg prison from Guantanamo Bay on the basis that, while both are located outside the sovereign territory of the United States, Guantanamo Bay is under the *exclusive* control of the United States, whereas Landsberg prison was under the control of the combined Allied Forces.[87] In an attempt at further reconciliation, Justice Kennedy noted that nothing in *Eisentrager* stated that *de jure* sovereignty has ever been the only consideration in determining the reach of the Constitution.[88] Justice Kennedy thus concluded that "a common thread" used to determine "questions of extraterritoriality turn on objective factors and practical concerns, not formalism[,]" and thus unites the *Insular cases, Eisentrager*, and *Reid*.[89]

However, as Justice Scalia pointed out in his dissent in *Boumediene*, the majority completely missed the mark with *Eisentrager*, which "conclusively establishes the opposite" of a functional test for extraterritoriality.[90] Quoting Justice Jackson in *Eisentrager*, Justice Scalia noted, "in extending constitutional protections beyond the citizenry, the Court has been at pains to point out that it was the alien's presence within its territorial jurisdiction that gave the judiciary power to act."[91] From the language in *Eisentrager*, Justice Scalia concluded that *Eisentrager* "*held* beyond any doubt - that the Constitution does not ensure habeas for aliens held by the United States in areas over which our Government is not sovereign."[92]

The *Insular cases*, *Reid*, and *Eisentrager*, do in fact stand for the same idea, as observed by the majority. However, the majority interpreted these cases incorrectly. Instead of standing for a functional approach to extraterritoriality, Justice Scalia pointed out that, like *Eisentrager*, the *Insular cases* stand for the proposition that aliens outside of United States sovereign territory do not have

---

[87] *Boumedien*, 553 U.S. at 768. The United States was therefore "answerable to its Allies" for all activities occurring at Landsberg prison. *Id.*

[88] *Boumediene*, 553 U.S. at 764.

[89] *Id.*

[90] *Id.* at 834 (Scalia, J., dissenting).

[91] *Boumedien*, 553 U.S. at 835 (Scalia, J., dissenting) (quoting *Eisentrager*, 339 U.S. at 770-71).

[92] *Boumediene*, 553 U.S. at 835 (Scalia, J., dissenting) (emphasis in original).

constitutional rights.[93] Quoting *Balzac v. Porto Rico*,[94] Justice Scalia stated that, "The Constitution of the United States is in force in Porto Rico as it is wherever and whenever the *sovereign power of that government is exerted*."[95] Moreover, all of the Justices of the *Reid* majority, save one, limited their analysis to the rights of citizens abroad.[96]

The *Insular cases* dealt with territory that was a part of the United States' sovereign territory,[97] the *Reid* Court addressed the rights of citizens abroad, and *Eisentrager* specifically declined to extend constitutional privileges to foreign nationals outside of United States sovereign territory. Functional approach or not, the idea that the Constitution applies to foreign nationals outside of the United States' sovereignty can not be found in any of the Supreme Court's previous opinions. Contrary to Justice Kennedy's ultimate holding in *Boumediene*, Justice Frankfurter stated in his concurrence that, while the "deck of a private American vessel . . . is considered for many purposes constructively as territory of the United States . . . persons on board such vessels . . . cannot invoke the protection of the provisions [of the Constitution] until brought within the actual territorial boundaries of the United States."[98] Thus, the functional *de jure* versus *de facto* sovereignty approach adopted by the majority in *Boumediene* is not only judicially created, but is a blatant misconstruction and revision of the Court's previous case law in a weak attempt at justification.

---

[93] *Boumediene*, 553 U.S. at 839 (Scalia, J., dissenting).

[94] 258 U.S. 298 (1922). Justice Kennedy cited this case in concluding that the *Insular Cases* created a functional test for the application of the Constitution to American territories. *See Boumediene*, 553 U.S. at 758.

[95] *Boumediene*, 553 U.S. at 839 (Scalia, J., dissenting) (quoting Balzac v. Porto Rico, 258 U.S. at 312.) (emphasis added).

[96] *Boumediene*, 553 U.S. at 839 (Scalia, J., dissenting). *See Reid*, 354 U.S. at 5-6 (plurality opinion of Black, J., Harlan, J., and Frankfurter, J., concurring in result). Justice Frankfurter was the only Justice in the majority that did not limit the analysis to American citizens abroad. However, Justice Frankfurter went a step further and limited his analysis to civilian dependents of American military abroad, an even narrower class.

[97] *See Boumediene*, 553. U.S. at 839; *Verdugo*, 494 U.S. at 268; *Reid,* 354 U.S. at 13 (plurality opinion of Black, J.).

[98] *Reid*, 354 U.S. at 55-6. (quoting In re Ross, 140 U.S. 453, 464 (1891).

Although *Boumediene* seems to have rewritten the *Insular* cases, *Reid*, and *Eisentrager*, and did not overrule *Verdugo* despite being in direct contradiction to it, it is still controlling law. Therefore, there is a rather gray area of law regarding the application of the Constitution to foreign national terror suspects held aboard American military vessels that are located in international waters. Under *Eisentrager* and *Verdugo*, the Fourth Amendment would not apply to the search of a foreign-national terrorism suspect, so long as the search occurs outside of the territory of the United States, where the United States lacks *de jure* sovereignty. Under *Boumediene*, however, the Fourth Amendment seemingly applies to a search of such foreign-national terrorism suspects if conducted within an area where the United States exercises *de facto* sovereignty through 'complete and total control,' in addition to searches conducted within the *de jure* sovereignty of the United States. While the *Eisentrager*/*Verdugo* and *Boumediene* rules may lead to the same result in some cases, such as if a search of a foreign-national terrorism suspect occurred within the sovereign territory of the United States, the same cannot be said when the search is conducted where the United States only exercises *de facto*, and not *de jure* sovereignty.

Such a situation is in fact presented by the handling of Ahmed Abu Khatallah by the United States Government. By searching Abu Khatallah on a military vessel in international waters, the United States searched Abu Khatallah in a location where the country certainly lacks *de jure* jurisdiction (by virtue of being in international waters), yet arguably exercises *de facto* jurisdiction (by virtue of being on an American military vessel). Applying the *Boumediene* holding to the actions of the Government in dealing with Abu Khatallah, his search would not be legal, absent a warrant, if the military vessel on which the search occurred can be equated to being under *de facto* sovereignty of the United States.

One significant question thus arises: was Ahmed Abu Khatallah within the 'complete and total control' of the United States when he was searched while being held on the American military ship in international waters? The answer to this question may dictate not only the legality of the Government's actions with Abu Khatallah, but also may impact the future course of conduct of the United

States in dealing with similarly-situated terrorism suspects that have been captured.

IV. DOES THE UNITED STATES EXERCISE *DE FACTO* SOVEREIGNTY OVER AMERICAN MILITARY SHIPS IN INTERNATIONAL WATERS?

In determining whether an American military vessel in international waters is equivalent to Guantanamo Bay for *Boumediene* purposes, several sources may help shed light on how the vessel should be treated. One such source is the United Nations Convention on the Law of the Sea.[99]

Designed to define the rights and responsibilities of nations regarding the world's oceans, the Convention on the Law of the Sea states that, "[s]hips have the nationality of the State whose flag they are entitled to fly,"[100] and that, "ships shall sail under the flag of one State only and . . . shall be subject to its exclusive jurisdiction on the high seas."[101] Additionally, the Convention goes further in specifying that warships on the high seas "have complete immunity from the jurisdiction of any State other than the flag State."[102] Lastly, the Convention mandates that every State shall "assume jurisdiction under its internal law over each ship flying its flag."[103]

Following the language in the Convention of the Law of the Sea and the rule laid down in *Boumediene*, a search of Ahmed Abu Khatallah aboard an American military ship in international waters would be subject to the restrictions of the Fourth Amendment.

---

[99] United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 243.

[100] United Nations Convention on the Law of the Sea art. 91, Dec. 10, 1982, 1833 U.N.T.S. 243.

[101] United Nations Convention on the Law of the Sea art. 92, Dec. 10, 1982, 1833 U.N.T.S. 243.

[102] United Nations Convention on the Law of the Sea art. 95, Dec. 10, 1982, 1833 U.N.T.S. 243.

[103] United Nations Convention on the Law of the Sea art. 94, Dec. 10, 1982, 1833 U.N.T.S. 243.

Because he was searched on an American military vessel, the ship carries the nationality of the United States and is subject to the exclusive jurisdiction of the United States. The "internal law" that the Convention subjects the ship to as an American vessel most certainly refers to the United States Constitution, including the provisions of the Fourth Amendment.

The provisions of the Convention on the Law of the Sea do not bind the United States because the United States has not become a signatory party to the Convention.[104] However, customary international law echoes the rule eventually adopted by the Convention on the Law of the Sea. Predating the Convention on the Law of the Sea, the Permanent Court of International Justice stated in *The Case of the S.S. "Lotus" (France v. Turkey)*[105] [*hereinafter* "the *Lotus* case"], "a ship on the high seas is assimilated to the territory of the State the flag of which it flies."[106] Furthermore, the *Lotus* case points out that "a ship is placed in the same position as national territory," and that "what occurs on board a vessel on the high seas must be regarded as if it occurred on the territory of the State whose flag the ship flies."[107]

While the U.N. Convention on the Law of the Sea may not bind the United States, the *Lotus* case does bind the United States absent conflicting domestic law.[108] Because neither Congress nor

---

[104] Int'l & Operational Law Dep't, The Judge Advocate Gen.'s Legal Ctr. & Sch., U.S. Army, JA 422, Operational Law Handbook, p. 163 (2014). *But see Id.* at n. 13 (describing support for US ratification, including support from former Presidents Bill Clinton and George W. Bush).

[105] *The Case of the S.S. "Lotus" (France v. Turkey)*, 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7).

[106] *The Case of the S.S. "Lotus" (France v. Turkey)*, 1927 P.C.I.J. (ser. A) No. 10, ¶ 65 (Sept. 7).

[107] *Id.*

[108] The Paquete Habana, 175 U.S. 677, 700 (1900) (holding that customary international law is binding on the United States in the absence of conflicting domestic law). On the other hand, courts have held that customary international law is not controlling where Congress has specifically enacted a law on the issue. *See* Echeverria-Hernandez v. INS, 923 F.2d 688, 694 (9th Cir. 1991), *vacated on other grounds,* 946 F.2d 1481 (1991) (holding that the customary norm of safe haven in times of civil war was preempted by the enactment of the Refugee Act of 1980 and the executive act of voluntary departure).

courts have directly dealt with the territorial characteristics of military vessels, The Commander's Handbook on the Law of Naval Operations is perhaps the most important tool in analyzing the way the United States Government views its military vessels, as well as the jurisdictional laws surrounding them. It is therefore helpful in determining whether an American military vessel can be equated to Guantanamo Bay for *Boumediene* purposes of applying the Constitution to foreign nationals.

According to the Commander's Handbook, which provides guidance for American military officers "on the rules of law governing naval operations in peacetime and during armed conflict,"[109] United States Naval policy *requires* warships to assert the rights of sovereign immunity.[110] The privilege of sovereign immunity entitles all U.S. warships and United States ships (USS) to "exclusive control over persons onboard such vessels with respect to acts performed onboard."[111] More importantly, the Commander's Handbook states, "U.S. law applies at all times aboard U.S. vessels as the law of the flag nation and is enforceable on U.S. vessels . . . anywhere in the world."[112]

Similar to the Commander's Handbook, the Judge Advocate General's Operational Law Handbook, which acts as a "how to" guide for military lawyers[113] declares that state craft, including warships, are "absolutely immune on the high seas."[114]

---

[109] Int'l Law Dep't, U.S. Naval War College, U.S. Navy, NWP 1-14M, The Commanders Handbook on the Law of Naval Operations, p. 3 (2007).

[110] Int'l Law Dep't, U.S. Naval War College, U.S. Navy, NWP 1-14M, The Commanders Handbook on the Law of Naval Operations, § 2.2.2, p. 2-2 (2007).

[111] Int'l Law Dep't, U.S. Naval War College, U.S. Navy, NWP 1-14M, The Commanders Handbook on the Law of Naval Operations, § 2.1, p. 2-1 (2007).

[112] Int'l Law Dep't, U.S. Naval War College, U.S. Navy, NWP 1-14M, The Commanders Handbook on the Law of Naval Operations, § 3.11.2.1, p. 3-10 (2007).

[113] Int'l & Operational Law Dep't, The Judge Advocate Gen.'s Legal Ctr. & Sch., U.S. Army, JA 422, Operational Law Handbook, p. i (2014).

[114] Int'l & Operational Law Dep't, The Judge Advocate Gen.'s Legal Ctr. & Sch., U.S. Army, JA 422, Operational Law Handbook, p. 174 (2014) (citing article

Both the Commander's Handbook and the Operational Law Handbook strongly suggest that American military ships in international waters are essentially United States territory abroad, and certainly under the exclusive control and jurisdiction of the United States. Both the Commander's Handbook and the Operational Law Handbook thus can be said to equate an American military ship in international waters to Guantanamo Bay, for *de facto* jurisdictional purposes. Similar to the *Boumediene* reasoning of "complete and total control" that the United States holds over Guantanamo Bay, the Commander's Handbook gives the United States "exclusive control" over military vessels such as the one used to transport Ahmed Abu Khatallah.

Moreover, the Commander's Handbook specifically states that U.S. law applies at all times on American flagged vessels. Surely, U.S. law refers to the whole Constitution including the Fourth Amendment. Therefore, the United States Government must abide by the Fourth Amendment when it searches terrorism suspects like Ahmed Abu Khatallah aboard an American military vessel, even if the vessel is located in international waters.

V. RAMIFICATIONS OF EXTENDING FOURTH AMENDMENT PROTECTIONS TO FOREIGN NATIONALS HELD ABOARD AMERICAN MILITARY SHIPS IN INTERNATIONAL WATERS.

The practice of extending the provisions of the Fourth Amendment to foreign nationals held aboard an American military vessel in international waters raises several important policy considerations. Firstly, who has the jurisdiction to issue warrants for such searches? Could any federal judge in the United States issue such a warrant? Or would it be limited to judges within a certain jurisdiction? And if so, which jurisdiction? Similarly, what court can hear challenges to such warrants? Would it be the district court to which the suspect is ultimately brought? Or would it be a special court created specifically for such purposes?

---

95 of the Convention of the Law of the Sea). *See also Id.* at 171 (providing complete sovereign immunity for State vessels).

The second policy consideration implicated by such a decision is what effect that decision will have on future dealings with captured terrorism suspects. The United States can easily defeat having to grant the protections of the Fourth Amendment to a foreign suspect by delaying the suspect from reaching an American vessel. Capturing forces could take the time to search and interrogate the suspect in the nation where the capture takes place before transporting the suspect back to the United States. However, this would result in added delay, and most likely added risk for both the capturing forces and the captured suspect, who would have to spend more time in a likely hostile environment. The consequences of extending the protections of the Fourth Amendment to foreign suspects aboard American ships in international waters could therefore result in a failure to even prevent a search of the suspect without a warrant, while at the same time place American citizens, and even the foreign suspect himself, at greater harm.

A third important policy consideration is the likelihood of compliance with such a rule. Compliance with such a rule ultimately relies on whether the information resulting from a search would later be used or excluded from the trial of the captured terrorism suspect. Exclusion of ill-gotten information would most likely help ensure compliance with the requirements of the Fourth Amendment. However, if the Government already has a strong enough case (and if the Government is going to exercise its rendition powers, it likely has a strong enough case already) then exclusion of the information resulting from the search would not be of much consequence. Searches would be conducted more for intelligence value rather than evidentiary value during a subsequent prosecution, and the threat of future exclusion of information gained would therefore not stop searches when a warrant is unable to be obtained. The rule requiring a warrant would thus prove toothless, all the while unnecessarily restricting the later prosecution of the captured suspect.

VI. CONCLUSION

While the history of decisions regarding the extraterritorial application of the Constitution, from *Eisentrager* to *Verdugo*, seems to

suggest that the United States Government's search of Ahmed Abu Khatallah aboard a ship in international waters is legal, the Supreme Court's decision in *Boumediene* challenges that theory.

Following the *Verdugo* holding and Justice Frankfurter's concurrence in *Reid*, the Fourth Amendment would not be applicable to foreign nationals held aboard American ships in international waters. However, following the more recent *Boumediene* holding, because the American military vessel on which he was searched is subject to the exclusive control and jurisdiction of the United States, despite being in international waters and outside United States territory, the protections of the Fourth Amendment would seemingly extend to Abu Khatallah just as the protections of a habeas corpus petition extended to the detainees held at Guantanamo Bay in *Boumediene*. In other words, the Fourth Amendment would protect Abu Khatallah because an American military ship in international waters is "not abroad; it is within the constant jurisdiction of the United States."[115]

Regardless of the lack of value and heavy burden produced by such a rule, in light of *Boumediene*, the Fourth Amendment, as well as the rest of the Constitution, likely applies to foreign terrorism suspects held aboard American military vessels, even if the ships are located in international waters. This unintended consequence of the *Boumediene* decision leaves the United States Government operating in a dubious zone of legality when it searches terrorist suspects aboard military vessels absent a warrant, and may ultimately necessitate a change in the way the United States deals with captured terrorism suspects in the future.

[115] *See Boumediene*, 553 U.S. 723 at 769; Rasul v. Bush, 542 U.S. 466, 480 (2004).